

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-069480
 (43)Date of publication of application : 16.03.2001

(51)Int.Cl. H04N 7/167
 H04H 1/00
 H04H 1/02
 H04L 9/08

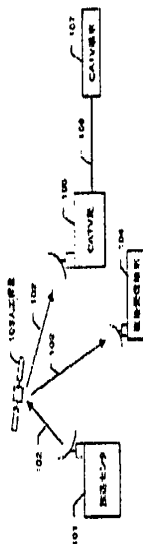
(21)Application number : 11-243916 (71)Applicant : MATSUSHITA ELECTRIC IND CO LTD
 (22)Date of filing : 30.08.1999 (72)Inventor : NAGATA MINEHISA
 KITA TERUhide
 SAKURAI ATSUNORI
 NAITO YASUFUMI
 GOTO YOSHIMASA

(54) CONDITIONAL ACCESS SYSTEM

(57)Abstract:

PROBLEM TO BE SOLVED: To provide a conditional access system where a repeater relays contents sent from a broadcast center without descrambling the contents with a simple configuration and the repeater can uniquely manage conditional access of a terminal.

SOLUTION: A broadcast center 101 transmits a 1st EMM together with contents, a 1st ECM including a same scramble key Ks, and a 2nd ECM, and a CATV station 105 multiplexes a 2nd EMM on a transport stream including the contents to relay the resulting stream to a CATV channel 106. A CATV terminal 107 discriminates viewing on the basis of the 2nd ECM and the 2nd EMM, extracts the key Ks and views the contents, then the CATV station 107 relays the contents with a simple configuration without the need for descrambling the contents and manages conditional access of the CATV terminal 107.



* NOTICES *

JPO and INPIT are not responsible for any damages caused by the use of this translation.

1. This document has been translated by computer. So the translation may not reflect the original precisely.
2. **** shows the word which can not be translated.
3. In the drawings, any words are not translated.

CLAIMS

[Claim(s)]

[Claim 1] A center apparatus, one or more repeating installation, and the first one or more terminal units are connected in the first transmission line, Said repeating installation and the second one or more terminal units are the conditional access systems connected, and in the second transmission line said center apparatus, Carry out the scramble of the contents containing either an image, a sound or data, and it sends out to said first transmission line, Encipher the first common information including the first access area judging that performs an access judging to a scramble key which carries out the scramble of said contents, and said contents, and it carries out multiplex to said contents, While enciphering the first individual information including contract information of the first work key that enciphers said first common information, and said first terminal unit and carrying out multiplex to said contents, Encipher the second common information including the second access area judging that performs an access judging to said scramble key and said contents with the second work key, and it carries out multiplex to said contents, While said repeating installation relays information containing said contents which received from said first transmission line to said second transmission line, Carry out multiplex to information which enciphers the second individual information including contract information of said second work key and said second terminal unit, and contains said contents, and it sends out to said second transmission line, Said first terminal unit on a basis the first access area judging contained in said first common information, and contract information included in said first individual information said second terminal unit, A conditional access system characterized by performing access control to said contents based on the second access area judging contained in said second common information, and contract information included in said second individual information.

[Claim 2] A center apparatus, one or more repeating installation, and the first one or more terminal units are connected in the first transmission line, Said repeating installation and the second one or more terminal units are connected in the second transmission line, Further, said center apparatus and said repeating installation are conditional access systems connected, and in the third transmission line said center apparatus, Carry out the scramble of the contents containing either an image, a sound or data, and it sends out to said first transmission line, Encipher the first common information including the first access area judging that performs an access judging to a scramble key which carries out the scramble of said contents, and said contents, and it carries out multiplex to said contents, While enciphering the first individual information including contract information of the first work key that enciphers said first common information, and said first terminal unit, carrying out multiplex to said contents and sending out to said first transmission line, Encipher the second common information including the second access area judging that performs an access judging to said scramble key and said contents with the second work key, and it sends out to said third transmission line, While relaying information containing said contents which received from said first transmission line to said second transmission line, said repeating installation said second common information received from said third transmission line, Carry out multiplex to information which carries out multiplex to information containing said contents, enciphers the second individual information including contract information of said second work key and said second terminal unit, and contains said contents, and it sends out to said second transmission line, Said first terminal unit on a basis the first access area judging contained in said first common information, and contract information included in said first individual information said second terminal unit, A conditional access system performing access control to said contents based on the second access area judging contained in said second common information, and contract information included in said second individual information.

[Claim 3] Whenever it changes said center apparatus, send it out once, and said second common information said repeating installation. The conditional access system according to claim 1 or 2 characterized by repeating and sending out said second common information with a constant interval until it will receive the second common information changed into the next, if said second common information is received.

[Claim 4] The conditional access system according to any one of claims 1 to 3, wherein said center apparatus enciphers said second common information with a cipher system other than a cipher system of said first common information.

[Claim 5] The conditional access system according to any one of claims 1 to 4, wherein said repeating installation enciphers said second individual information with a cipher system other than a cipher system of said first individual information that said center apparatus performs.

[Claim 6] The conditional access system according to any one of claims 1 to 5 Tia's describing the first access area judging of said first common information, and describing the second access area judging of said second common information by a channel bit map.

[Claim 7] The conditional access system according to any one of claims 1 to 5 a channel bit map's describing the first access area judging of said first common information, and describing the second access area judging of said second common information by Tia.

[Claim 8] The conditional access system according to any one of claims 1 to 7, wherein said center apparatus stores and sends out said scramble key to said second common information, and said repeating installation receives said second common information and adds and sends out an access area judging.

[Claim 9] Said center apparatus stores said scramble key in said second common information, enciphers and sends it out with said second work key, and said repeating installation. While the third work key enciphers and sends out a field including said second common information that received said second common information, added an access area judging and was received, and said added access area judging. The conditional access system according to any one of claims 1 to 7 storing and sending out said second work key and said third work key to said second individual information.

[Claim 10] The conditional access system according to any one of claims 1 to 9, wherein said repeating installation removes and relays said first common information that exists in information containing said contents which received from said first transmission line.

[Claim 11] The conditional access system according to any one of claims 2 to 9, wherein said repeating installation replaces and relays said first common information that exists in information containing said contents which received from said first transmission line, and said second common information received from said third transmission line.

[Claim 12] Said center apparatus carries out multiplex [of the empty information] to said contents suitably, sends it out to said first transmission line, and said repeating installation. From said first transmission line, remove said first individual information and information containing said contents which received is relayed. The conditional access system according to any one of claims 1 to 11 replacing and carrying out multiplex [of information and said second individual information of said empty which exists in information containing said contents].

[Claim 13] The conditional access system according to any one of claims 1 to 11, wherein said repeating installation replaces and carries out multiplex [of said first individual information that exists in information containing said contents which received from said first transmission line, and said second individual information].

[Claim 14] The conditional access system according to any one of claims 1 to 11, wherein said repeating installation carries out frequency multiplexing of said second individual information to a frequency band other than a frequency band from which information containing said contents is relayed and sends it out to it.

[Claim 15] Said repeating installation and said second terminal unit are connected even in fourth transmission line where said second transmission line is another, and said repeating installation,

Relay information containing said contents to said second transmission line, send out said second individual information to said fourth transmission line, and to it said second terminal unit. The conditional access system according to any one of claims 1 to 11 performing access control to said contents based on the second received common information and the second individual information received from said fourth transmission line from said second transmission line.

[Claim 16] In said second common information, said contents provide a program attribute which shows the Tia program or a pay-per-view program, and to it it said center apparatus, Store, send out the Tia information and pay-per-view information to the second access area judging in said second common information, and said repeating installation, responding to employment -- said program attribute of said second common information -- either the Tia program or a pay-per-view program -- or, The conditional access system according to any one of claims 1 to 15, wherein it changes into a value which shows both and said second terminal unit judges access control by Tia, pay-per-view either, or both with reference to said program attribute.

[Claim 17] The conditional access system according to any one of claims 1 to 16 sending said second work key to said repeating installation with a storage from said center apparatus.

[Claim 18] The conditional access system according to any one of claims 1 to 16 transmitting said second work key to said repeating installation from said center apparatus in the first transmission line.

[Claim 19] The conditional access system according to any one of claims 1 to 16 transmitting said second work key to said repeating installation from said center apparatus in the third transmission line.

[Claim 20] The conditional access system according to any one of claims 1 to 16 transmitting said second work key to said repeating installation using a public network from said center apparatus.

[Claim 21] The conditional access system according to any one of claims 16 to 20, wherein it sends said second work key to said center apparatus with a storage from said one certain repeating installation and said center apparatus sends said second received work key to said other repeating installation.

[Claim 22] Two-way communication is possible for said first transmission line, and said second work key is transmitted to said center apparatus from said one certain repeating installation in said first transmission line. The conditional access system according to any one of claims 16 to 20, wherein said center apparatus sends said second received work key to said other repeating installation.

[Claim 23] Two-way communication is possible for said third transmission line, and said second work key is transmitted to said center apparatus from said one certain repeating installation in said third transmission line. The conditional access system according to any one of claims 16 to 20, wherein said center apparatus sends said second received work key to said other repeating installation.

[Claim 24] The conditional access system according to any one of claims 16 to 20, wherein it transmits said second work key to said center apparatus using a public network from said one certain repeating installation and said center apparatus sends said second received work key to said other repeating installation.

[Claim 25] The conditional access system according to any one of claims 17 to 24, wherein said center apparatus or said repeating installation enciphers and transmits said second work key using a private key cryptosystem.

[Claim 26] The conditional access system according to any one of claims 17 to 24, wherein said center apparatus or said repeating installation enciphers and transmits said second work key using a public-key crypto system.

[Claim 27] Store, send out said center apparatus to said second common information if needed, and a telephone number of the first viewing history collection place said repeating installation. The conditional access system according to any one of claims 1 to 22, wherein it stores and sends out a telephone number of the second viewing history collection place to said second individual information if needed and said terminal unit transmits a viewing history, using preferentially a

telephone number of said first viewing history collection place.

[Claim 28] A common information stripper which is a common information stripper belonging to the conditional access system according to claim 1 or 2, and is characterized by said common information stripper removing said first common information from information which is installed in said repeating installation and contains said contents.

[Claim 29] Said first common information of information containing said contents which it is a common information multiplexer belonging to the conditional access system according to claim 2, and said common information multiplexer was installed in said repeating installation, and received from said first transmission line, A common information multiplexer replacing said second common information received from said third transmission line.

[Claim 30] An individual information stripper which is an individual information stripper belonging to the conditional access system according to claim 1 or 2, and is characterized by said individual information stripper removing said first individual information from information which is installed in said repeating installation and contains said contents.

[Claim 31] An individual information multiplexer which is an individual information multiplexer belonging to the conditional access system according to claim 1 or 2, and is characterized by said individual information multiplexer replacing said first individual information in information which is installed in said repeating installation and contains said contents, and said second individual information.

[Claim 32] A common information multiplexer which is a common information multiplexer belonging to the conditional access system according to claim 3, and is characterized by sending out said common information multiplexer repeatedly until it receives the second common information changed into the next in said second common information it was installed in said repeating installation and received.

[Translation done.]

* NOTICES *

JPO and INPIT are not responsible for any damages caused by the use of this translation.

1. This document has been translated by computer. So the translation may not reflect the original precisely.
2. **** shows the word which can not be translated.
3. In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]

[0001]

[Field of the Invention] This invention relates to the limited reception method for performing the reception control of a terminal unit to the signal which relayed signals, such as satellite broadcasting, via the transmission line of CATV etc., or a system.

[0002]

[Description of the Prior Art] Generally in satellite broadcasting etc., the passthrough method etc. are known as a method of transmitting the signal by which scramble was carried out as it is, without performing descrambling and re-scramble by a CATV station etc., and performing limited reception.

[0003] The method of SAIMARU crypto is known as a method of making two or more limited

reception intermingled to one contents.

[0004] Hereafter, a Prior art is explained using figures.

[0005] Drawing 40 is a figure showing the important section of the system configuration of a passthrough method.

[0006] CATV station 4009 is connected with the satellite center 4001 by the satellite connection using the satellite 4008, and the terminal unit 4015 is connected with CATV station 4009 with the CATV network. * NOTICES *

JPO and INPIT are not responsible for any damages caused by the use of this translation.

1. This document has been translated by computer. So the translation may not reflect the original precisely.
2. **** shows the word which can not be translated.
3. In the drawings, any words are not translated.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]

[Drawing 1] The entire configuration figure of the conditional access system in a 1st embodiment of this invention,

[Drawing 2] The internal configuration figure of the broadcast center in a 1st embodiment of this invention,

[Drawing 3] The internal configuration figure of the CATV station in a 1st embodiment of this invention,

[Drawing 4] The internal configuration figure of the direct reception terminal in a 1st embodiment of this invention,

[Drawing 5] The internal configuration figure of the CATV terminal in a 1st embodiment of this invention,

[Drawing 6] The basic constitution figure of EMM in a 1st embodiment of this invention,

[Drawing 7] The basic constitution figure of ECM in a 1st embodiment of this invention,

[Drawing 8] The figure showing operation of the limited reception module in a 1st embodiment of this invention,

[Drawing 9] The lineblock diagram of the viewing-and-listening judging TIA bit in a 1st embodiment of this invention,

[Drawing 10] The lineblock diagram of the contract information TIA bit in a 1st embodiment of this invention,

[Drawing 11] The lineblock diagram of the viewing-and-listening judging bit map in a 1st embodiment of this invention,

[Drawing 12] The lineblock diagram of the contract information bit map in a 1st embodiment of this invention,

[Drawing 13] The internal configuration figure of the multiplex section in a 2nd embodiment of this invention,

[Drawing 14] The figure showing the important section of the header unit of an MPEG 2 transport stream packet,

[Drawing 15] The basic constitution figure of ECM in a 2nd embodiment of this invention,

[Drawing 16] The internal configuration figure of the multiplex section in a 3rd embodiment of this invention,

[Drawing 17] The basic constitution figure of EMM in a 3rd embodiment of this invention,

[Drawing 18] The figure showing operation of the multiplexer in a 3rd embodiment of this invention,

[Drawing 19] The internal configuration figure of the multiplex section in a 4th embodiment of this invention,
 [Drawing 20] The figure showing operation of the individual information multiplexer in a 4th embodiment of this invention,
 [Drawing 21] The internal configuration figure of the multiplex section in a 5th embodiment of this invention,
 [Drawing 22] The figure showing operation of the common information multiplexer in a 5th embodiment of this invention,
 [Drawing 23] The lineblock diagram of the second ECM in a 5th embodiment of this invention,
 [Drawing 24] The lineblock diagram of the second ECM in a 6th embodiment of this invention,
 [Drawing 25] The lineblock diagram of the second ECM in a 6th embodiment of this invention,
 [Drawing 26] The lineblock diagram of the second EMM in a 6th embodiment of this invention,
 [Drawing 27] The internal configuration figure of the CATV station in a 7th embodiment of this invention,
 [Drawing 28] The figure showing the frequency band on the CATV circuit in a 7th embodiment of this invention,
 [Drawing 29] The internal configuration figure of the CATV terminal in a 7th embodiment of this invention,
 [Drawing 30] The internal configuration figure of the CATV station in an 8th embodiment of this invention,
 [Drawing 31] The internal configuration figure of the CATV terminal in an 8th embodiment of this invention,
 [Drawing 32] The internal configuration figure of the broadcast center in a 9th embodiment of this invention,
 [Drawing 33] The inside of the multiplex section of the CATV station in a 9th embodiment of this invention, and a surrounding lineblock diagram,
 [Drawing 34] The figure showing operation of the common information multiplexer in a 9th embodiment of this invention,
 [Drawing 35] The entire configuration figure of the conditional access system in a 10th embodiment of this invention,
 [Drawing 36] The figure showing operation of the CATV terminal in a 10th embodiment of this invention,
 [Drawing 37] The entire configuration figure of the conditional access system in an 11th embodiment of this invention,
 [Drawing 38] The internal configuration figure of the broadcast center in an 11th embodiment of this invention,
 [Drawing 39] The internal configuration figure of the second CATV station in an 11th embodiment of this invention,
 [Drawing 40] The figure explaining the conventional passthrough method,
 [Drawing 41] It is a figure explaining the conventional SAIMARU crypto method.
 [Description of Notations]
 101, 3701 broadcast centers
 104 and 3702 Direct reception terminal
 105 CATV station
 107 CATV terminal
 202 and 3803 First EMM generation part
 204 and 3804 First ECM generation part
 205, 3202, and 3806 Second ECM generation part
 206, 3201, and 3805 Second Kw Management Department
 207, 3203, and 3809 SAIMARU crypto control section

303, 2703, a 3903 PSI converter
 304 and 3904 Multiplex section
 305, 2704, a 3905 QAM modulation part
 306, 2705, and 3906 Frequency conversion part
 307, 2706, and 3001 Second Kw Management Department
 308, 2707, and 3002 Second EMM generation part
 404, 504, 2904, and 3104 Separation part
 405, 505, 2905, and 3105 Limited reception module
 1301 Common information stripper
 1302, 1602, 2102, and 3302 Multiplexer
 1501 ECM identifier
 1601 Individual information stripper
 1701 EMM identifier
 1901 Individual information multiplexer
 2101 and 3301 Common information multiplexer
 2301 Program attribute
 2710 Modulation part
 2708 Frequency conversion part
 2901 Distribution part
 2909 The second EMM extraction part
 3003 Communications department
 3101 Communications department
 3204 Communications department
 3303 Communications department
 3501 The first viewing history collection center
 3502 The second viewing history collection center
 3703 The first CATV station
 3705 The first CATV terminal
 3706 The second CATV station
 3708 The second CATV terminal
 3907 Nth Kw Management Department
 3908 The Nth EMM generation part

[Translation done.]

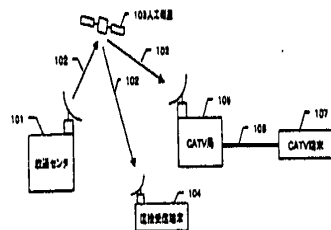
* NOTICES *

JPO and INPIT are not responsible for any damages caused by the use of this translation.

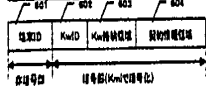
1. This document has been translated by computer. So the translation may not reflect the original precisely.
2. **** shows the word which can not be translated.
3. In the drawings, any words are not translated.

DRAWINGS

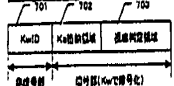
[Drawing 1]



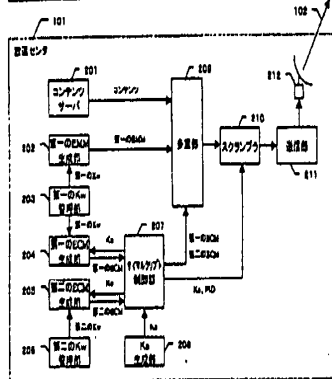
[Drawing 6]



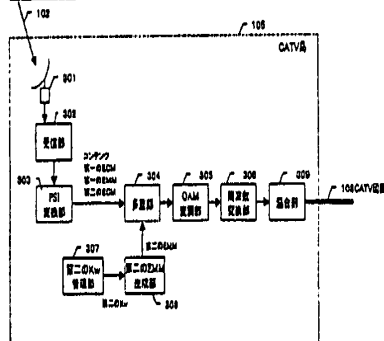
[Drawing 7]



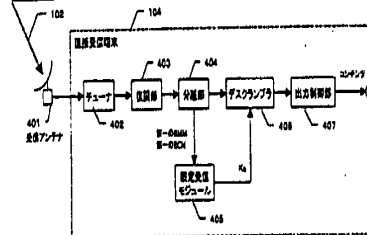
[Drawing 2]



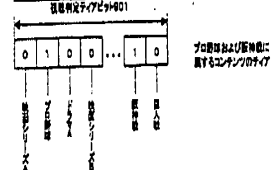
[Drawing 3]



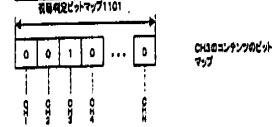
[Drawing 4]



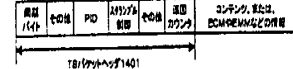
[Drawing 9]



[Drawing 11]



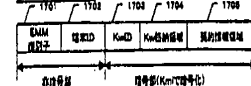
[Drawing 14]



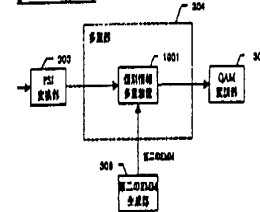
[Drawing 15]



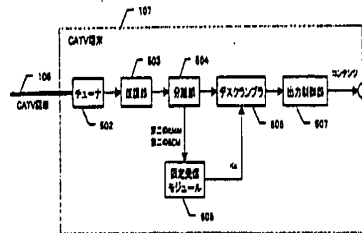
[Drawing 17]



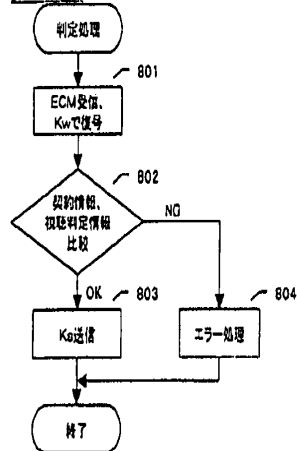
[Drawing 19]



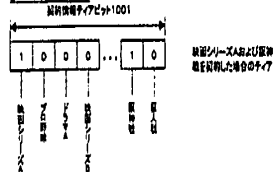
[Drawing 5]



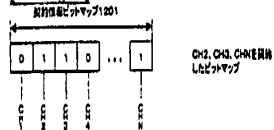
[Drawing 8]



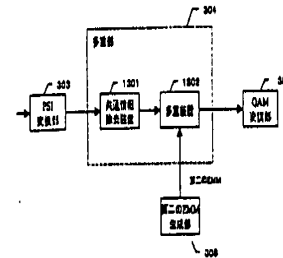
[Drawing 10]



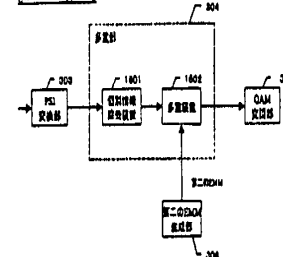
[Drawing 12]



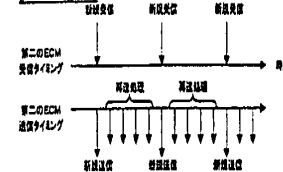
[Drawing 13]



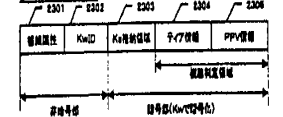
[Drawing 16]



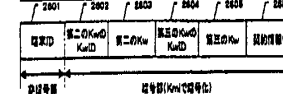
[Drawing 22]



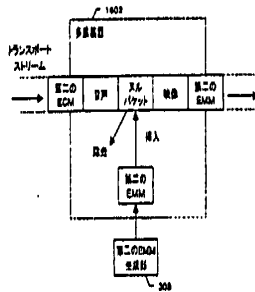
[Drawing 23]



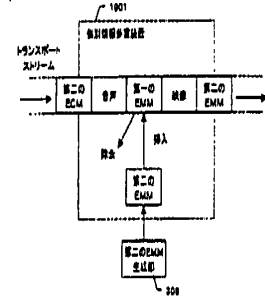
[Drawing 26]



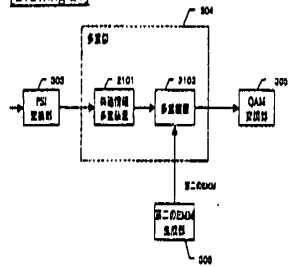
[Drawing 18]



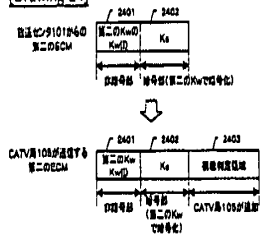
[Drawing 20]



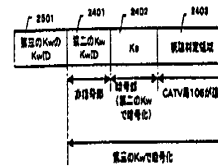
[Drawing 21]



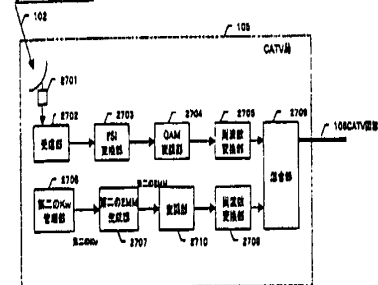
[Drawing 24]



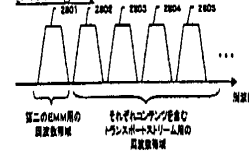
[Drawing 25]



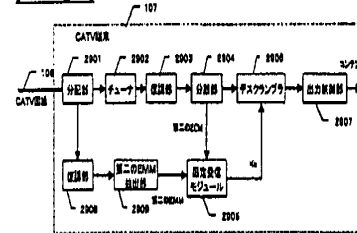
[Drawing 27]



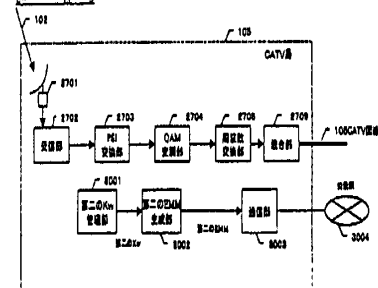
[Drawing 28]



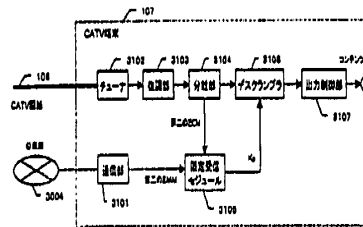
[Drawing 29]



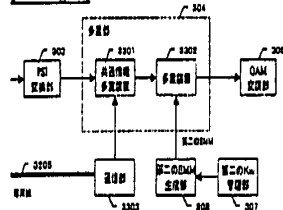
[Drawing 30]



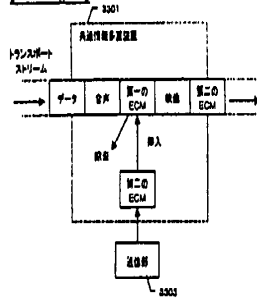
[Drawing 31]



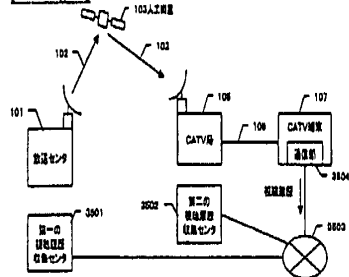
[Drawing 33]



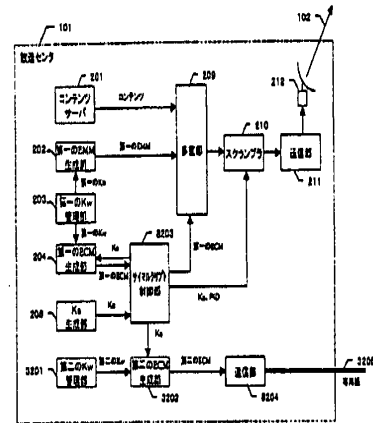
[Drawing 34]



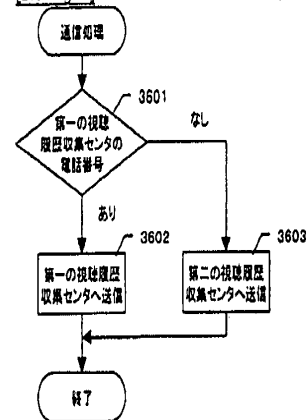
[Drawing 35]



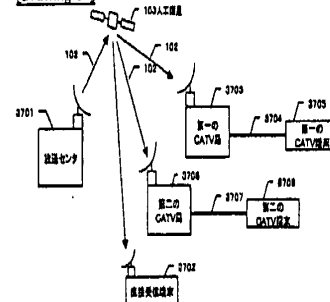
[Drawing 32]



[Drawing 36]



[Drawing 37]



[Drawing 38]

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号
特開2001-69480
(P2001-69480A)

(43) 公開日 平成13年3月16日 (2001.3.16)

(51) Int. Cl. ⁷	識別記号	F I	テロパ ⁷ (参考)
H04N 7/167		H04N 7/167	Z 5C064
H04H 1/00		H04H 1/00	U 5J104
	1/02	1/02	E
H04L 9/08		H04L 9/00	601A
			601E

審査請求 未請求 請求項の範囲 OL (全 30 頁)

(21) 出願番号	特願平11-243916	(71) 出願人	00005821 松下電器産業株式会社 大阪府門真市大字門真1006番地
(22) 出願日	平成11年8月30日 (1999.8.30)	(72) 発明者	永田 峰久 大阪府門真市大字門真1006番地 松下電器 産業株式会社内
		(72) 発明者	北 岡秀 大阪府門真市大字門真1006番地 松下電器 産業株式会社内
		(74) 代理人	100193254 弁理士 豊 昌明 (外3名)

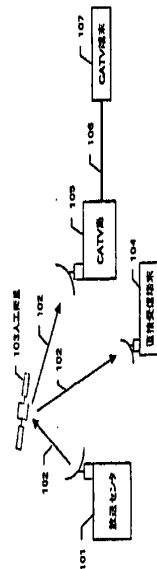
最終頁に続く

(54) (発明の名称) 限定受信システム

(57) (要約)

【課題】 放送センタから送信されるコンテンツを、中継装置においてデスクランブルせずに、簡単な構成で中継し、しかも中継装置が独自に端末装置の限定受信の管理可能な限定受信システムを提供する。

【解決手段】 放送センタ100からコンテンツとともに第一のECMと、同一のスクランブル鍵Ksを含む第一のECM及び第二のECMを送信し、CATV局105は上記コンテンツを含むトランスポートストリームK、第二のECMを多重してCATV回線106へ中継する。CATV局107は第二のECM及び第二のECMを基にして復調判定を行い、Ksを取り出し、コンテンツを復調するようにしたので、CATV局107では、コンテンツをデスクランブルする必要がなく簡単な構成で中継でき、さらにCATV局107の限定受信の管理を行うことができる。



(2)

特開2001-69480

2

【特許請求の範囲】

【請求項1】 センタ装置と1つ以上の中継装置及び1つ以上の第一の端末装置とが第一の伝送路で接続され、前記中継装置と1つ以上の第二の端末装置とが第二の伝送路で接続される限定受信システムであって、

前記センタ装置は、映像、音声またはデータなどのいずれかを含むコンテンツをスクランブルして前記第一の伝送路へ送出し、前記コンテンツをスクランブルするスクランブル鍵及び前記コンテンツへのアクセス判定を行う第一のアクセス判定

領域を含む第一の共通情報を暗号化して前記コンテンツに多重し、前記第一の共通情報を暗号化する第一のワーク鍵及び前記第一の端末装置の契約情報を含む第一の個別情報を暗号化して前記コンテンツに多重するとともに、前記スクランブル鍵及び前記コンテンツへのアクセス判定を行う第二のアクセス判定領域を含む第二の共通

情報を第二のワーク鍵で暗号化して前記コンテンツに多重し、前記中継装置は、前記第一の伝送路から受信した前記コンテンツを含む情報

を前記第二の伝送路へ中継するとともに、前記第二のワーク鍵及び前記第二の端末装置の契約情報を含む第二の個別情報を暗号化して前記コンテンツに多重して前記第二の伝送路へ送出し、

前記第一の端末装置は、前記第一の共通情報に含まれる第一のアクセス判定領域と前記第一の個別情報に含まれる契約情報とを基に、また、前記第二の共通情報に含まれる第二のアクセス判定領域と前記第二の個別情報に含まれる契約情報とを基に、前記コンテンツへのアクセス制御を行うことを特徴とする限定受信システム。

【請求項2】 センタ装置と1つ以上の中継装置及び1つ以上の第一の端末装置とが第一の伝送路で接続され、前記中継装置と1つ以上の第二の端末装置とが第二の伝送路で接続され、前記センタ装置と前記中継装置とはさらに第三の伝送路で接続される限定受信システムであって、

前記センタ装置は、映像、音声またはデータなどのいずれかを含むコンテンツをスクランブルして前記第一の伝送路へ送出し、前記コンテンツをスクランブルするスクランブル鍵及び前記コンテンツへのアクセス判定を行う第一のアクセス判定領域を含む第一の共通情報を暗号化して前記コンテンツに多重し、前記第一の共通情報を暗号化する第一のワーク鍵及び前記第一の端末装置の契約情報を含む第一の個別情報を暗号化して前記コンテンツに多重して前記第一の伝送路へ送出するとともに、前記スクランブル鍵及び前記コンテンツへのアクセス判定を行う第二のアクセス判定領域を含む第二の共通情報を第二のワーク鍵で暗号化して前記第二の伝送路へ送出し、

前記中継装置は、前記第一の伝送路から受信した前記コンテンツを含む情報を前記第二の伝送路へ中継するとともに、前記第二のワーク鍵及び前記第二の端末装置の契約情報を含む第二の個別情報を暗号化して前記コンテンツに多重して前記第二の伝送路へ送出し、

前記第一の端末装置は、前記第一の共通情報に含まれる第一のアクセス判定領域と前記第一の個別情報に含まれる契約情報とを基に、また、前記第二の共通情報に含まれる第二のアクセス判定領域と前記第二の個別情報に含まれる契約情報とを基に、前記コンテンツへのアクセス制御を行うことを特徴とする限定受信システム。

【請求項3】 前記センタ装置は、前記第二の共通情報を、変更するたびに一度送出し、前記中継装置は、前記第二の共通情報を受信すると、次に変更された第二の共通情報を受信するまで、前記第二の共通情報を一定間隔で繰り返し送出することを特徴とする請求項1または2に記載の限定受信システム。

【請求項4】 前記センタ装置は、前記第一の共通情報の暗号化方式とは別の暗号化方式で前記第二の共通情報を暗号化することを特徴とする請求項1から3のいずれかに記載の限定受信システム。

【請求項5】 前記中継装置は、前記センタ装置が行う前記第一の個別情報の暗号化方式とは別の暗号化方式で前記第二の個別情報を暗号化することを特徴とする請求項1から4のいずれかに記載の限定受信システム。

【請求項6】 前記第一の共通情報の第一のアクセス判定領域はチャネルビットマップで記述することと特徴とする請求項1から5のいずれかに記載の限定受信システム。

【請求項7】 前記第一の共通情報の第一のアクセス判定領域はチャネルビットマップで記述し、前記第二の共通情報の第二のアクセス判定領域はチャネルビットマップで記述することを特徴とする請求項1から6のいずれかに記載の限定受信システム。

前記中継装置は、前記第一の伝送路から受信した前記コンテンツを含む情報を前記第二の伝送路へ中継するとともに、前記第二の伝送路から受信した前記第二の共通情報を、前記コンテンツを含む情報に多重し、前記第二のワーク鍵及び前記第二の端末装置の契約情報を含む第二の個別情報を暗号化して前記コンテンツに多重して前記第二の伝送路へ送出し、

前記第一の端末装置は、前記第一の共通情報に含まれる第一のアクセス判定領域と前記第一の個別情報に含まれる契約情報とを基に、また、前記第二の共通情報に含まれる第二のアクセス判定領域と前記第二の個別情報に含まれる契約情報とを基に前記コンテンツへのアクセス制御を行うことを特徴とする限定受信システム。

【請求項8】 前記センタ装置は、前記第二の共通情報を、変更するたびに一度送出し、前記中継装置は、前記第二の共通情報を受信すると、次に変更された第二の共通情報を受信するまで、前記第二の共通情報を一定間隔で繰り返し送出することを特徴とする請求項1または2に記載の限定受信システム。

【請求項9】 前記センタ装置は、前記第一の共通情報の暗号化方式とは別の暗号化方式で前記第二の共通情報を暗号化することを特徴とする請求項1から3のいずれかに記載の限定受信システム。

【請求項10】 前記中継装置は、前記センタ装置が行う前記第一の個別情報の暗号化方式とは別の暗号化方式で前記第二の個別情報を暗号化することを特徴とする請求項1から4のいずれかに記載の限定受信システム。

【請求項11】 前記第一の共通情報の第一のアクセス判定領域はチャネルビットマップで記述することと特徴とする請求項1から5のいずれかに記載の限定受信システム。

【請求項12】 前記第一の共通情報の第一のアクセス判定領域はチャネルビットマップで記述し、前記第二の共通情報の第二のアクセス判定領域はチャネルビットマップで記述することを特徴とする請求項1から6のいずれかに記載の限定受信システム。

【請求項13】 前記センタ装置は、前記第二の共通情報を、変更するたびに一度送出し、前記中継装置は、前記第二の共通情報を受信すると、次に変更された第二の共通情報を受信するまで、前記第二の共通情報を一定間隔で繰り返し送出することを特徴とする請求項1または2に記載の限定受信システム。

【請求項14】 前記センタ装置は、前記第一の共通情報の暗号化方式とは別の暗号化方式で前記第二の共通情報を暗号化することを特徴とする請求項1から3のいずれかに記載の限定受信システム。

【請求項15】 前記中継装置は、前記センタ装置が行う前記第一の個別情報の暗号化方式とは別の暗号化方式で前記第二の個別情報を暗号化することを特徴とする請求項1から4のいずれかに記載の限定受信システム。

【請求項16】 前記第一の共通情報の第一のアクセス判定領域はチャネルビットマップで記述することと特徴とする請求項1から5のいずれかに記載の限定受信システム。

【請求項17】 前記第一の共通情報の第一のアクセス判定領域はチャネルビットマップで記述し、前記第二の共通情報の第二のアクセス判定領域はチャネルビットマップで記述することを特徴とする請求項1から6のいずれかに記載の限定受信システム。

【請求項18】 前記センタ装置は、前記第二の共通情報を、変更するたびに一度送出し、前記中継装置は、前記第二の共通情報を受信すると、次に変更された第二の共通情報を受信するまで、前記第二の共通情報を一定間隔で繰り返し送出することを特徴とする請求項1または2に記載の限定受信システム。

【請求項19】 前記センタ装置は、前記第一の共通情報の暗号化方式とは別の暗号化方式で前記第二の共通情報を暗号化することを特徴とする請求項1から3のいずれかに記載の限定受信システム。

【請求項20】 前記中継装置は、前記センタ装置が行う前記第一の個別情報の暗号化方式とは別の暗号化方式で前記第二の個別情報を暗号化することを特徴とする請求項1から4のいずれかに記載の限定受信システム。

前記第二の個別情報に前記第二のワーク鍵及び前記第三のワーク鍵を格納して送出することを特徴とする請求項1から7のいずれかに記載の限定受信システム。

【請求項10】 前記中継装置は、前記第一の伝送路から受信した前記コンテンツを含む情報に存在する前記第一の共通情報を取り除いて中継することを特徴とする請求項1から9のいずれかに記載の限定受信システム。

【請求項11】 前記中継装置は、前記第一の伝送路から受信した前記コンテンツを含む情報に存在する前記第一の共通情報と、前記第三の伝送路から受信した前記第二の共通情報とを入れ替えて中継することを特徴とする請求項2から8のいずれかに記載の限定受信システム。

【請求項12】 前記センタ装置は、前記コンテンツに適宜空の情報を多重して前記第一の伝送路へ送出し、前記中継装置は、前記第一の伝送路から受信した前記コンテンツを含む情報を、前記第一の個別情報を取り除いて中継し、前記コンテンツを含む情報に存在する前記空の情報と前記第二の個別情報とを入れ替えて多重することとを特徴とする請求項1から11のいずれかに記載の限定受信システム。

【請求項13】 前記中継装置は、前記第一の伝送路から受信した前記コンテンツを含む情報に存在する前記第一の個別情報と、前記第二の個別情報とを入れ替えて多重することとを特徴とする請求項1から11のいずれかに記載の限定受信システム。

【請求項14】 前記中継装置は、前記コンテンツを含む情報を中継する周波数帯域とは別の周波数帯域に、前記第二の個別情報を周波数多重して送出することを特徴とする請求項1から11のいずれかに記載の限定受信システム。

【請求項15】 前記中継装置と前記第二の端末装置とは、前記第二の伝送路とは別の第四の伝送路でも接続されており、前記中継装置は、前記コンテンツを含む情報を前記第二の伝送路に中継し、前記第二の個別情報を前記第四の伝送路へ送出し、前記第二の端末装置は、前記第二の伝送路から受信した第二の共通情報と、前記第四の伝送路から受信した第二の個別情報とに基づいて、前記コンテンツへのアクセス制御を行うことを特徴とする請求項1から11のいずれかに記載の限定受信システム。

【請求項16】 前記第二の共通情報に、前記コンテンツがティア番組かハイパー番組かを示す番組属性を設け、前記センタ装置は、前記第二の共通情報における第二のアクセス判定領域にティア情報及びハイパー番組情報を格納して送出し、前記中継装置は、通用に応じて、前記第二の共通情報の前記番組属性をティア番組またはハイパー番組のいずれか、若しくは、両方を示す値に変更し、前記第二の端末装置は、前記番組属性を参照して、アクセス制御の判定をティアまたはハイパー番組のいずれか、若しくは、両方で行うことを特

徴とする請求項1から15のいずれかに記載の限定受信システム。

【請求項17】 前記第二のワーク鍵を前記センタ装置から前記中継装置へ配線媒体で送ることを特徴とする請求項1から16のいずれかに記載の限定受信システム。

【請求項18】 前記第二のワーク鍵を前記センタ装置から前記中継装置へ第一の伝送路にて伝送することを特徴とする請求項1から16のいずれかに記載の限定受信システム。

10 【請求項19】 前記第二のワーク鍵を前記センタ装置から前記中継装置へ第三の伝送路にて伝送することを特徴とする請求項1から16のいずれかに記載の限定受信システム。

【請求項20】 前記第二のワーク鍵を前記センタ装置から前記中継装置へ公衆網を用いて伝送することを特徴とする請求項1から16のいずれかに記載の限定受信システム。

20 【請求項21】 前記第二のワーク鍵をある1つの前記中継装置から前記センタ装置へ配線媒体で送り、前記センタ装置は受け取った前記第二のワーク鍵をその他の前記中継装置へ送ることを特徴とする請求項1から20のいずれかに記載の限定受信システム。

【請求項22】 前記第一の伝送路は双方向通信可能であって、前記第二のワーク鍵をある1つの前記中継装置から前記センタ装置へ前記第一の伝送路にて伝送し、前記センタ装置は受け取った前記第二のワーク鍵をその他の前記中継装置へ送ることを特徴とする請求項1から20のいずれかに記載の限定受信システム。

30 【請求項23】 前記第三の伝送路は双方向通信可能であって、前記第二のワーク鍵をある1つの前記中継装置から前記センタ装置へ前記第三の伝送路にて伝送し、前記センタ装置は受け取った前記第二のワーク鍵をその他の前記中継装置へ送ることを特徴とする請求項1から20のいずれかに記載の限定受信システム。

【請求項24】 前記第二のワーク鍵をある1つの前記中継装置から前記センタ装置へ公衆網を用いて伝送し、前記センタ装置は受け取った前記第二のワーク鍵をその他の前記中継装置へ送ることを特徴とする請求項1から20のいずれかに記載の限定受信システム。

40 【請求項25】 前記センタ装置または前記中継装置は、前記第二のワーク鍵を、秘密鍵暗号方式を用いて暗号化を行い、伝送することを特徴とする請求項17から24のいずれかに記載の限定受信システム。

【請求項26】 前記センタ装置または前記中継装置は、前記第二のワーク鍵を、公開鍵暗号方式を用いて暗号化を行い、伝送することを特徴とする請求項17から24のいずれかに記載の限定受信システム。

【請求項27】 前記センタ装置は、必要に応じて前記第二の共通情報に第一の視聴履歴収集先の電話番号を格

納して送出し、前記中継装置は、必要に応じて前記第二

の個別情報に第二の視聴履歴収集先の電話番号を格納して送出し、前記端末装置は、前記第一の視聴履歴収集先の電話番号を優先的に使用して視聴履歴を送信することを特徴とする請求項1から22のいずれかに記載の限定受信システム。

【請求項28】 請求項1または2に記載の限定受信システムに属する共通情報多重装置であって、前記共通情報多重装置は前記中継装置に設置され、前記コンテンツを含む情報から前記第一の共通情報を取り除くことを特徴とする共通情報多重装置。

【請求項29】 請求項2に記載の限定受信システムに属する共通情報多重装置であって、前記共通情報多重装置は前記中継装置に設置され、前記第一の伝送路から受信した前記コンテンツを含む情報の前記第一の共通情報と、前記第三の伝送路から受信した前記第二の共通情報とを入れ替えることを特徴とする共通情報多重装置。

【請求項30】 請求項1または2に記載の限定受信システムに属する個別情報多重装置であって、前記個別情報多重装置は前記中継装置に設置され、前記コンテンツを含む情報から前記第一の個別情報を取り除くことを特徴とする個別情報多重装置。

【請求項31】 請求項1または2に記載の限定受信システムに属する個別情報多重装置であって、前記個別情報多重装置は前記中継装置に設置され、前記コンテンツを含む情報における前記第一の個別情報と、前記第二の個別情報とを入れ替えることを特徴とする個別情報多重装置。

【請求項32】 請求項3に記載の限定受信システムに属する共通情報多重装置であって、前記共通情報多重装置は前記中継装置に設置され、受信した前記第二の共通情報を、次に変更された第二の共通情報を受信するまで、繰り返し送出することを特徴とする共通情報多重装置。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、衛星放送などの信号をCATVなどの伝送路を介して中継した信号に対する端末装置の受信制御を行うための限定受信方法またはシステムに関するものである。

【0002】

【従来の技術】衛星放送などにおいて、スクランブルされた信号を、CATV局などでデスクランブル、再スクランブルを行わずに、そのまま伝送して限定受信を行う方法としては、一般に、バスループ方式などが知られている。

【0003】また、1つのコンテンツに対して2つ以上の限定受信を課せさせる方法として、サイマルクリプトという方法が知られている。

【0004】以下、図を用いて従来の技術を説明する。

【0005】図4はバスループ方式のシステム構成の

要部を示す図である。

【0006】衛星センタ4001とCATV局4009が衛星4008を利用した衛星回線と接続され、CATV局4009と端末装置4015がCATV網と接続されている。

【0007】衛星を通じてコンテンツを送信する衛星センタ4001は、映像や音声などを含むコンテンツを送出するコンテンツサーバ4002と、コンテンツをスクランブルするための情報やそれを復号化するための情報（ECM、EMM）を送出する限定受信制御部4004と、コンテンツとECMやEMMとを多重化したストリームを生成する多重部4003と、ストリームの指定されたコンテンツをスクランブルするスクランブラ4005と、ストリームを衛星回線に伝じた変調などの送信処理を行う送信部4006と、復調されたストリームを衛星回線へ送出する送信アンテナ4007とを具備している。

【0008】また、衛星から受信したコンテンツをCATV網へ送出するCATV局4009は、衛星回線からストリームを受信する受信アンテナ4010と、受信したストリームに復調などの受信処理を行う受信部4011と、番組情報（PSI）を衛星伝送用途からケーブル伝送用途に交換するPSI変換部4012と、復調したデータをCATVで規定されているQAM方式に変調するQAM変調器4013と、ストリームをCATVの伝送周波数に変換してCATV網へ送出する周波数変換部4014とを具備している。

【0009】このシステムの衛星センタ4001では、コンテンツサーバ4002が多重部4003へ映像や音声などを含むコンテンツを送信する。また、限定受信制御部4004は、コンテンツに対する視聴許可を判定するための判定領域とコンテンツをスクランブルしたスクランブル鍵（Ks）とを持つ共通情報（ECM）をワーク鍵（Kw）で暗号化して多重部4003へ送信し、また、各端末装置4015に対してコンテンツへの視聴許可を与える契約情報領域とECMを暗号化したKwとを持つ個別情報（EMM）を、各端末装置4015に固有の個別鍵（Km1）で暗号化して多重部4003へ送信し、さらに、スクランブラ4005に対して、スクランブルを行うコンテンツを識別するための識別子（PID）とスクランブル鍵（Ks）とを送信する。

40 【0010】多重装置4003は、受信したコンテンツとECM及びEMMとを1つのストリームに多重してスクランブラ4005へ送信し、スクランブラ4005は、受信したストリームのうち限定受信制御部4004により指定されたPIDを持つコンテンツに対してスクランブルを行い、送信部4006へ送信する。送信部4006はストリームを衛星回線に伝じた変調などの送信処理を行い、送信アンテナ4007を介して衛星回線へ送出する。

【0011】CATV局4009では、受信部4011が受信アンテナ4010を介して衛星回線からストリームを受信し、復調などの受信処理を行いPSI変換部4012へ送信す

る。PSI変換部4012では、番組記列情報(PSI)の一部であり、突頭周波数などの伝送路の情報とコンテンツとを関連付ける情報を伝送するためのNITを、衛星伝送用途からケーブル伝送用途に変換してQAM変換部4013へ送信し、QAM変換部4013はCATVで規定されているQAM方式に変換して周波数変換部4014へ送信し、周波数変換部4014はストリームをCATVの伝送周波数に変換してCATV網へ送出する。

【0012】端末装置4015は、CATV網からストリームを受信し、自分宛のEMMを復号し、契約情報及びKwを保持し、スクランブルされたコンテンツを視聴する場合には、まず、該コンテンツに付随するECMを受信してKwで復号し、ECM内の判定領域と契約情報とを比較し視聴許可の有無を調べる。視聴許可が有りと判定されれば、ECM内のKsを用いて該コンテンツをデスクランブルすることができ、視聴可能となる。

【0013】以上のように、バススルー方式においては、CATV局4009では単にストリームをCATV網に送った変調方式などに交換するのみであり、ECMやEMMを復号する必要もなく、その内容には関与せずに中継することができる。この方式では、各端末装置4015の契約管理は全て衛星センタ4001が行う。

【0014】また、図41は、同一のコンテンツに対して複数の限定受信を課金させるサイマルクリプト方式のシステム構成の要部を示す図である。図41において、コンテンツ、ECM、EMMなどの関係は上記で説明したのと同等である。

【0015】放送センタ4101は、第一の限定受信方式に属する端末装置に対するEMMを生成する第一のEMM生成装置4103と、第二の限定受信方式に属する端末装置に対するEMMを生成する第二のEMM生成装置4104と、第一の限定受信方式のECMを生成する第一のECM生成装置4105と、第二の限定受信方式のECMを生成する第二のECM生成装置4106と、映像や音声などで構成されるコンテンツを送出するコンテンツサーバ4102と、コンテンツと第一及び第二のEMM並びにECMとを多重する多重部4109と、コンテンツをスクランブルするためのKsを一定間隔で生成するKs生成装置4108と、第一及び第二のECMを多重部4109へ出力し、PIDとKsとをスクランブル4110へ出力するサイマルクリプト制御部4107と、スクランブルを実行するスクランブラ4110と、ストリームを突頭処理して端末装置4112へ送出する送信部4111とを備えている。

【0016】このシステムの放送センタ4101では、コンテンツサーバ4102が映像や音声などで構成されるコンテンツを多重部4109へ送信する。第一のEMM生成装置4103は、第一の限定受信方式に属する各端末装置4112に対して、コンテンツへの視聴許可を与える契約情報領域を含む第一のEMMを多重部4109へ送信し、第二のEMM生成装置4104は、第二の限定受信方式に属する各端末装

置4112に対して上記と同一のコンテンツへの視聴許可を与える契約情報領域を含む第二のEMMを多重部4109へ送信する。また、Ks生成装置4108はコンテンツをスクランブルするためのKsを一定間隔で生成し、サイマルクリプト制御部4107へ送信する。サイマルクリプト制御部4107は、受信したKsを第一のECM生成装置4105及び第二のECM生成装置4106へ送信し、第一のECM生成装置4105は、コンテンツに対する視聴許可を判定するための判定領域と受信したKsとを含む第一のECMを生成し、サイマルクリプト制御部4107へ送信し、第二のECM生成装置4106は、上記と同一のコンテンツに対する視聴許可を判定するための判定領域と受信したKsとを含む第二のECMを生成し、サイマルクリプト制御部4107へ送信する。

【0017】サイマルクリプト制御部4107は、受信した第一のECM及び第二のECMを多重部4109へ送信するとともに、スクランブルを行うコンテンツを識別するPIDとKsとをスクランブラ4110へ送信する。多重部4109は、コンテンツ、第一のECM、第二のECM、第一のEMM及び第二のEMMを多重して1つのストリームとしてスクランブラ4110へ送信し、スクランブラ4110は、指定されたPIDとKsとを基に、該当するコンテンツに対してスクランブルを行い、送信部4111へ送信する。送信部4111は、このストリームに伝送路に適した突頭処理などを行い伝送路へ送出する。

【0018】第一の限定受信方式に属する端末装置4112は、ストリームから自分宛の第一のEMMを受信し、契約情報を保持し、コンテンツに付随する第一のECMの判定領域と契約情報とを比較し、視聴許可が有りと判定されれば該コンテンツのデスクランブルを行うことができ視聴可能となる。また、第二の限定受信方式に属する端末装置4112は、ストリームから自分宛の第二のEMMを受信し、契約情報を保持し、コンテンツに付随する第二のECMの判定領域と契約情報とを比較し、視聴許可が有りと判定されれば該コンテンツのデスクランブルを行うことができ視聴可能となる。

【0019】このように、サイマルクリプト方式を用いれば、同一のコンテンツに対して複数の限定受信を課金させることが可能となる。

【0020】さらに、上記で説明したバススルー方式とサイマルクリプト方式とを組み合わせると簡単に柔軟な限定受信が可能となる。すなわち、図40における衛星センタ4001と図41における放送センタ4101とを同一と見なすと、衛星センタ4001において複数の限定受信を課金させることが可能となり、CATV局4009ではそれぞれのECM、EMMには関与せずに中継する。このようにすれば、例えば、コンテンツを衛星センタ4001から衛星回線を通して直接受信するような直接受信端末がある場合に、直接受信端末には第一の限定受信方式を利用し、CATV局4009に接続される端末装置4015は第二

の限定受信方式を利用することによって、衛星センタ4001とCATV局4009は独立してそれぞれの端末の限定受信を実現することが可能となる。

【0021】

【発明が解決しようとする課題】しかし、上記のように従来の技術を組み合わせた方法では、CATV局が管理すべき端末装置に対するEMMを、衛星センタに設置される第二のEMM生成装置が生成し送出する。この場合には、CATV局が管理する端末装置の契約情報またはEMMそのものをCATV局から衛星センタに通知する必要があるため、契約情報の秘匿性の低下が懸念される。

【0022】また、システムの形態によっては、数万の端末装置を管理するCATV局が複数あることも想定され、この場合には、衛星センタから送出される第二のEMMの伝送容量が大幅に増大する可能性がある。現在のデジタル放送では1つの放送周波数帯域の伝送容量は約30Mbpsであり、第二のEMMの伝送容量が増大することは、コンテンツの伝送容量が縮小されることであるので、コンテンツの画質の低下やチャンネル数の削減などといった影響を及ぼす恐れもある。また、この場合に第二のEMMの伝送容量の増大を抑えればコンテンツに影響は及ばなくなるが、第二のEMMが帯域制限されたことで第二のEMM全てを送出するのに必要な時間が増え、各端末装置の契約情報が即時に反映されなくなり、顧客が視聴したいコンテンツをすぐに視聴できないといった影響を及ぼす可能性もある。

【0023】本発明は、こうした課題を解決するものであり、センタ装置からのコンテンツを中継する中継装置において、コンテンツをデスクランブルすることなく、ECMやEMMを復号することなく中継し、コンテンツに影響を及ぼさず、中継装置独自の限定受信を行うことができる限定受信システムを提供し、また、そのシステムを構成する装置を提供することを目的としている。

【0024】

【課題を解決するための手段】第1の発明は、センタ装置と1つ以上の中継装置及び1つ以上の第一の端末装置とが第一の伝送路で接続され、中継装置と1つ以上の第二の端末装置が第二の伝送路で接続される限定受信システムであって、センタ装置は、映像や音声などを含むコンテンツをスクランブルして第一の伝送路へ送出し、コンテンツをスクランブルするスクランブル装置及びコンテンツへのアクセス判定を行うアクセス判定領域を含む第一の共通情報を暗号化してコンテンツに多重し、第一の共通情報を暗号化する第一のワーク鍵及び第一の端末装置の契約情報を含む第一の個別情報を暗号化してコンテンツに多重するとともに、スクランブル装置及びアクセス判定領域を含む第二の共通情報を第二のワーク鍵で暗号化してコンテンツに多重し、中継装置は、第一の伝送路か

ら受信したコンテンツを含む情報を第二の伝送路へ中継するとともに、第二のワーク鍵及び第二の端末装置の契約情報を含む第二の個別情報を暗号化してコンテンツを含む情報に多重して第二の伝送路へ送出し、第一の端末装置は、第一の共通情報に含まれるアクセス判定領域と第一の個別情報に含まれる契約情報とを基に、また、第二の端末装置は、第二の共通情報に含まれるアクセス判定領域と第二の個別情報に含まれる契約情報とを基にコンテンツへのアクセス制御を行うという手段を有している。

【0025】以上のように第1の発明では、センタ装置がコンテンツ及び第一の個別情報とともに、コンテンツをスクランブルしたスクランブル装置を第一の共通情報及び第二の共通情報に含めて送出し、中継装置は受信したコンテンツ、第一の個別情報、第一の共通情報及び第二の共通情報を復号することなく中継するとともに、第二の個別情報を多重して送出するようにしたので、中継装置に接続される第二の端末装置に対して、センタ装置からのコンテンツを簡単に構成で提供でき低コスト化が図れるとともに、中継装置独自の限定受信を行うことができる。

【0026】第2の発明は、センタ装置と1つ以上の中継装置及び1つ以上の第一の端末装置とが第一の伝送路で接続され、中継装置と1つ以上の第二の端末装置とが第二の伝送路で接続され、センタ装置と中継装置とはさらに第三の伝送路で接続される限定受信システムであって、センタ装置は、映像、音声またはデータなどのいずれかを含むコンテンツをスクランブルして第一の伝送路へ送出し、コンテンツをスクランブルするスクランブル装置及びコンテンツへのアクセス判定を行う第一のアクセス判定領域を含む第一の共通情報を暗号化してコンテンツに多重し、第一の共通情報を暗号化する第一のワーク鍵及び第一の端末装置の契約情報を含む第一の個別情報を暗号化してコンテンツに多重して第一の伝送路へ送出するとともに、スクランブル装置及びコンテンツへのアクセス判定を行う第二のアクセス判定領域を含む第二の共通情報を第二のワーク鍵で暗号化して第三の伝送路へ送出し、中継装置は、第一の伝送路から受信したコンテンツを含む情報を第二の伝送路へ中継するとともに、第三の伝送路から受信した第二の共通情報を、コンテンツを含む情報に多重し、第二のワーク鍵及び第二の端末装置の契約情報を含む第二の個別情報を暗号化してコンテンツに多重して第二の伝送路へ送出し、第一の端末装置は、第一の共通情報に含まれる第一のアクセス判定領域と第一の個別情報に含まれる契約情報とを基に、また、第二の端末装置は、第二の共通情報に含まれる第二のアクセス判定領域と第二の個別情報に含まれる契約情報とを基にコンテンツへのアクセス制御を行うという手段を有している。

【0027】以上のように第2の発明では、センタ装置

が第二の共通情報を第三の伝送路へ送出し、中継装置が第二の共通情報及び第二の個別情報を、コンテンツを含む情報に多重するようにしたので、第一の伝送路上に、第一の端末装置には不要な第二の共通情報がないので、第一の端末装置の動作防止につながる。また、中継装置は、コンテンツや第二のECMを特にデスクランブルや復号を行わずに第二の伝送路へ送信できるので、簡単な構成で、第二の端末装置へコンテンツを提供することができ、低コスト化が図れるという効果が得られる。

【0028】第3の発明は、センタ装置は、第二の共通情報を、変更するたびに一度送出し、中継装置は、第二の共通情報を受信し、次に変更された第二の共通情報を受信するまで第二の共通情報を一定間隔で繰り返し送出するという手段を有している。

【0029】以上のように第3の発明では、中継装置が第二の共通情報の繰り返し送出を行うようにしたので、第一の伝送路上のコンテンツなどの伝送容量を増加させることが可能となり、コンテンツの更なる高画質化や、多チャンネル化といった効果が得られる。

【0030】第4の発明は、センタ装置は、第一の共通情報の符号化方式とは別の符号化方式で第二の共通情報を符号化するという手段を有している。

【0031】以上のように第4の発明では、第一の共通情報と第二の共通情報の符号化方式を別々の方式で行うので、第一の端末装置及び第二の端末装置に対する限定受信を更に独立して行うことが可能となり、一方の符号化方式が破られた場合にも、もう一方の限定受信には影響を及ぼすことがないという効果が得られる。

【0032】第5の発明は、中継装置は、センタ装置が行う第一の個別情報の符号化方式とは別の符号化方式で第二の個別情報を符号化するという手段を有している。

【0033】以上のように第5の発明では、第一の個別情報と第二の個別情報の符号化方式を別々の方式で行うので、第一の端末装置及び第二の端末装置に対する限定受信を更に独立して行うことが可能となり、一方の符号化方式が破られた場合にも、もう一方の限定受信には影響を及ぼすことがないという効果が得られる。

【0034】第6の発明は、第一の共通情報のアクセス判定領域はティアで記述し、第二の共通情報のアクセス判定領域はチャンネルビットマップで記述するという手段を有している。

【0035】以上のように第6の発明では、第一の共通情報と第二の共通情報のアクセス判定領域の構成を別々にしているため、第一の端末装置及び第二の端末装置に対する限定受信を更に独立して行うことが可能となり、一方のアクセス判定領域の構成が見破られて改竄された場合にも、もう一方の限定受信には影響を及ぼすことがないという効果が得られる。

【0036】第7の発明は、第一の共通情報のアクセス判定領域はチャンネルビットマップで記述し、第二の共

通情報のアクセス判定領域はティアで記述するという手段を有している。

【0037】以上のように第7の発明では、第一の共通情報と第二の共通情報のアクセス判定領域の構成を別々にしているため、第一の端末装置及び第二の端末装置に対する限定受信を更に独立して行うことが可能となり、一方のアクセス判定領域の構成が見破られて改竄された場合にも、もう一方の限定受信には影響を及ぼすことがないという効果が得られる。

【0038】第8の発明は、センタ装置は、第二の共通情報にスクランブル鍵を格納して送出し、中継装置は、第二の共通情報を受信し、アクセス判定領域を追加して送出するという手段を有している。

【0039】以上のように第8の発明では、センタ装置が第二の共通情報にスクランブル鍵を格納して送出し、中継装置が第二の共通情報にアクセス判定領域を追加して中継するので、第二の端末装置に対する限定受信を更に独立して行うことが可能となるという効果が得られる。

【0040】第9の発明は、センタ装置は、第二の共通情報にスクランブル鍵を格納し第二のワーク鍵で符号化して送出し、中継装置は、第二の共通情報を受信し、アクセス判定領域を追加し、受信した第二の共通情報及び追加したアクセス判定領域を含む領域を第三のワーク鍵で符号化して送出するとともに、第二の個別情報に第二のワーク鍵及び第三のワーク鍵を格納して送出するという手段を有している。以上のように第9の発明では、センタ装置が第二の共通情報にスクランブル鍵を格納して送出し、中継装置が第二の共通情報にアクセス判定領域を追加し、更に第三のワーク鍵で、アクセス判定領域を含めた第二の共通情報全体を符号化して送出し、第二の個別情報に第二のワーク鍵とともに第三のワーク鍵を含めて送出するようにしたので、第二の端末装置に対する限定受信をさらに独立して行うことが可能となるとともに、第二の共通情報の秘匿性を確保できるという効果が得られる。

【0041】第10の発明は、中継装置は、第一の伝送路から受信したコンテンツを含む情報に存在する第一の共通情報を取り除いて中継するという手段を有している。

【0042】以上のように第10の発明では、中継装置が第一の共通情報を取り除いて中継するようにしたので、第二の伝送路に送出する情報の伝送容量を増加できるという効果が得られる。

【0043】第11の発明は、中継装置は、第一の伝送路から受信したコンテンツを含む情報に存在する第一の共通情報と、第三の伝送路から受信した第二の共通情報を入れ替えて中継するという手段を有している。

【0044】以上のように第11の発明では、中継装置が第二の共通情報を第一の共通情報と入れ替えて送信す

るようにしたので、第一の伝送路上のコンテンツを含む情報の伝送容量を増やすことなく第二の伝送路に中継できるという効果が得られる。第12の発明は、センタ装置はコンテンツに適宜空の情報を多重して第一の伝送路へ送出し、中継装置は第一の伝送路から受信したコンテンツを含む情報を、第一の個別情報を取り除いて中継し、コンテンツを含む情報に存在する空の情報と第二の個別情報とを入れ替えて多重するという手段を有している。

【0045】以上のように第12の発明では、中継装置が第一の個別情報を取り除いて中継し、第二の情報を空の情報と入れ替えて送出するようにしたので、第二の伝送路に送出する情報の伝送容量を増加できるという効果が得られる。

【0046】第13の発明は、中継装置は第一の伝送路から受信したコンテンツを含む情報に存在する第一の個別情報と、第二の個別情報とを入れ替えて多重するという手段を有している。

【0047】以上のように第13の発明では、中継装置が第二の個別情報を受信する際に、第一の個別情報と入れ替えて送出するようにしたので、第一の伝送路上のコンテンツを含む情報の伝送容量を増やすことなく第二の伝送路に中継できるという効果が得られる。

【0048】第14の発明では、中継装置は、コンテンツを含む情報を中継する周波数帯域とは別の周波数帯域に、第二の個別情報を周波数多重して送出するという手段を有している。

【0049】以上のように第14の発明では、中継装置は、コンテンツを含む情報を中継する周波数帯域とは別の周波数帯域で第二の個別情報を伝送するようにしたので、コンテンツを含む情報の伝送容量に影響を及ぼすことなく、任意の伝送容量で第二の個別情報を伝送できるという効果が得られる。

【0050】第15の発明では、中継装置と第二の端末装置は、第二の伝送路とは別の第四の伝送路でも接続されており、中継装置は、コンテンツを含む情報を第二の伝送路に中継し、第二の個別情報を第四の伝送路に送出し、第二の端末装置は第二の伝送路から受信した第二の共通情報と、第四の伝送路から受信した第二の個別情報とに基づいて、コンテンツへのアクセス制御を行うという手段を有している。以上のように第15の発明では、中継装置と第二の端末装置を第二の伝送路及び第四の伝送路で接続し、中継装置はコンテンツを含む情報を第二の伝送路に中継し、第二の個別情報を第四の伝送路に送出するようにしたので、コンテンツを含む情報の伝送容量に影響を及ぼすことなく、任意の伝送容量で第二の個別情報を伝送できるという効果が得られる。

【0051】第16の発明では、第二の共通情報に、コンテンツがティア番組かペイパービュー番組を示す番組属性を設け、センタ装置は第二の共通情報のアクセス

判定領域にティア情報及びペイパービュー情報を格納して送出し、中継装置は適用に応じて任意に第二の共通情報の番組属性をティア番組またはペイパービュー番組のいずれか、若しくは、両方を示す値に変更し、第二の端末装置は番組属性を参照して、アクセス制御の判定をティアまたはペイパービューのいずれか、若しくは、両方で行うという手段を有している。

【0052】以上のように第16の発明では、第二の共通情報に、該コンテンツがティア番組かペイパービュー番組かを示す番組属性を設け、センタ装置は、第二の共通情報のアクセス判定領域にティア情報及びペイパービュー情報を格納して送出し、中継装置が適用に応じて任意に番組属性を変更して中継するようにしたので、第二の端末装置に対する限定受信を更に独立して行うことができるという効果が得られる。

【0053】第17の発明では、第二のワーク鍵をセンタ装置から中継装置へ記憶媒体で送るという手段を有している。

【0054】以上のように第17の発明では、第二のワーク鍵をセンタ装置から中継装置へ記憶媒体で送るようにしたので、簡単で確実に第二のワーク鍵を共有できるという効果が得られる。

【0055】第18の発明では、第二のワーク鍵をセンタ装置から中継装置へ第一の伝送路にて伝送するという手段を有している。

【0056】以上のように第18の発明では、第二のワーク鍵をセンタ装置から中継装置へ第一の伝送路にて伝送するようにしたので、任意のタイミングで第二のワーク鍵を変更でき、即時に共有できるという効果が得られる。

【0057】第19の発明では、第二のワーク鍵をセンタ装置から中継装置へ第三の伝送路にて伝送するという手段を有している。

【0058】以上のように第19の発明では、第二のワーク鍵をセンタ装置から中継装置へ第三の伝送路にて伝送するようにしたので、任意のタイミングで第二のワーク鍵を変更でき、即時に共有できるという効果が得られる。

【0059】第20の発明では、第二のワーク鍵をセンタ装置から中継装置へ公衆網を用いて伝送するという手段を有している。

【0060】以上のように第20の発明では、第二のワーク鍵をセンタ装置から中継装置へ公衆網を用いて伝送するようにしたので、任意のタイミングで第二のワーク鍵を変更でき、即時に共有できるという効果が得られる。

【0061】第21の発明では、第二のワーク鍵をある1つの中継装置からセンタ装置へ記憶媒体で送り、センタ装置は受け取った第二のワーク鍵をその他の中継装置へ送るという手段を有している。

【0082】以上のように第21の発明では、第二のワーク鍵をある1つの中継装置からセンタ装置へ記憶媒体で送り、更にセンタ装置から第二のワーク鍵をその他の中継装置へ送るようにしたので、簡単に確実に第二のワーク鍵を共有でき、中継装置が主体的に第二のワーク鍵の変更を行うことができるという効果が得られる。

【0083】第22の発明では、第一の伝送路は双方向通信可能であって、第二のワーク鍵をある1つの中継装置からセンタ装置へ第一の伝送路にて伝送し、センタ装置は受け取った第二のワーク鍵をその他の中継装置へ送るという手段を有している。以上のように第22の発明では、第二のワーク鍵をある1つの中継装置からセンタ装置へ第一の伝送路にて伝送し、センタ装置は第二のワーク鍵をその他の中継装置へ送るようにしたので、任意のタイミングで第二のワーク鍵を変更でき、即時に共有でき、中継装置が主体的に第二のワーク鍵の変更を行うことができるという効果が得られる。

【0084】第23の発明では、第三の伝送路は双方向通信可能であって、第二のワーク鍵をある1つの中継装置からセンタ装置へ第三の伝送路にて伝送し、センタ装置は受け取った第二のワーク鍵をその他の中継装置へ送るという手段を有している。以上のように第23の発明では、第二のワーク鍵をある1つの中継装置からセンタ装置へ第三の伝送路にて伝送し、センタ装置は第二のワーク鍵をその他の中継装置へ送るようにしたので、任意のタイミングで第二のワーク鍵を変更でき、即時に共有でき、中継装置が主体的に第二のワーク鍵の変更を行うことができるという効果が得られる。

【0085】第24の発明では、第二のワーク鍵をある1つの中継装置からセンタ装置へ公衆網を用いて伝送し、センタ装置は受け取った第二のワーク鍵をその他の中継装置へ送るという手段を有している。

【0086】以上のように第24の発明では、第二のワーク鍵をある1つの中継装置からセンタ装置へ公衆網を用いて伝送し、センタ装置は第二のワーク鍵をその他の中継装置へ送るようにしたので、任意のタイミングで第二のワーク鍵を変更でき、即時に共有でき、中継装置が主体的に第二のワーク鍵の変更を行うことができるという効果が得られる。

【0087】第25の発明では、センタ装置または中継装置は、第二のワーク鍵を秘密鍵暗号方式を用いて暗号化を行い、伝送するという手段を有している。

【0088】以上のように第25の発明では、センタ装置または中継装置が第二のワーク鍵を、秘密鍵を用いて暗号化を行い、伝送するようにしたので、第二のワーク鍵を安全に共有することができるという効果が得られる。

【0089】第26の発明では、センタ装置または中継装置は第二のワーク鍵を、公開鍵暗号方式を用いて暗号化を行い、伝送するという手段を有している。

【0070】以上のように第26の発明では、センタ装置または中継装置が第二のワーク鍵を、公開鍵を用いて暗号化を行い、伝送するようにしたので、第二のワーク鍵を安全に共有することができるという効果が得られる。

【0071】第27の発明では、センタ装置は、必要に応じて第二の共通情報に第一の視聴履歴収集先の電話番号を格納して送出し、中継装置は、必要に応じて第二の個別情報に第二の視聴履歴収集先の電話番号を格納して送出し、端末装置は、第一の視聴履歴収集先の電話番号を優先的に使用して視聴履歴を送信するという手段を有している。

【0072】以上のように第27の発明では、センタ装置が必要に応じて第二の共通情報に第一の視聴履歴収集先の電話番号を格納して送出し、中継装置は、必要に応じて第二の個別情報に第二の視聴履歴収集先の電話番号を格納して送出し、端末装置は第一の視聴履歴収集先の電話番号を優先的に使用して視聴履歴を送信するようにしたので、任意の視聴履歴収集先で視聴履歴を収集することができるという効果が得られる。

【0073】第28の発明では、共通情報除去装置は中継装置に設置され、コンテンツを含む情報から第一の共通情報を取り除くという手段を有している。

【0074】以上のように第28の発明では、共通情報除去装置が、コンテンツを含む情報から第一の共通情報を取り除くようにしたので、第二の伝送路上に第二の端末装置には不要な第一の共通情報がなくなるので、第二の端末装置の誤作動防止につながるという効果が得られる。

【0075】第29の発明では、共通情報多重装置は中継装置に設置され、第一の伝送路から受信したコンテンツを含む情報の第一の共通情報と、第三の伝送路から受信した第二の共通情報とを入れ替えるという手段を有している。

【0076】以上のように第29の発明では、共通情報多重装置が、第一の伝送路から受信したコンテンツを含む情報の第一の共通情報と、第三の伝送路から受信した第二の共通情報とを入れ替えるようにしたので、第一の伝送路上のコンテンツを含む情報の伝送容量を増やすことなく第二の伝送路に中継できるという効果が得られる。

【0077】第30の発明では、個別情報除去装置は中継装置に設置され、コンテンツを含む情報から第一の個別情報を取り除くという手段を有している。

【0078】以上のように第30の発明では、個別情報除去装置が、コンテンツを含む情報から第一の個別情報を取り除くようにしたので、第二の伝送路に送出する情報の伝送容量を増加でき、第二の端末装置には不要な第一の個別情報がなくなるので、第二の端末装置の誤作動防止につながるという効果が得られる。

【0079】第31の発明では、個別情報多重装置は中継装置に設置され、コンテンツを含む情報における第一の個別情報と、第二の個別情報とを入れ替えるという手段を有している。

【0080】以上のように第31の発明では、個別情報多重装置がコンテンツを含む情報における第一の個別情報と、第二の個別情報とを入れ替えて送信するようにしたので、第一の伝送路上のコンテンツを含む情報の伝送容量を増やすことなく第二の伝送路に中継できるという効果が得られる。

【0081】第32の発明では、共通情報多重装置は中継装置に設置され、受信した第二の共通情報を、次に変更された第二の共通情報を受信するまで、繰り返し送出するという手段を有している。

【0082】以上のように第32の発明では、共通情報多重装置が、受信した第二の共通情報を受信するまで、繰り返し送出するようにしたので、第一の伝送路上のコンテンツなどの伝送容量を増加させることが可能となり、コンテンツの更なる高画質化や、多チャンネル化といった効果が得られる。

【0083】

【発明の実施の形態】以下、本発明の実施の形態について、図面を用いて説明する。なお、本発明はこれらの実施の形態に何ら限定されるものではなく、その要旨を逸脱しない範囲において、種々なる態様で実施し得る。

【0084】(第1の実施の形態) 第1の実施形態では、限定受信システムの一例である、衛星放送をCATV局で中継して放送するデジタル放送システムについて説明する。

【0085】図1は、本実施形態における限定受信システムの全体構成を示すブロック図である。

【0086】放送センタ101とCATV局105は人工衛星103を利用した衛星回線102で接続され、また、放送センタ101と直接受信端末104は衛星回線102で接続される。更にCATV局105とCATV端末107はCATV回線106で接続される。

【0087】放送センタは放送電波を衛星回線102に送出し、直接受信端末104は衛星回線102から直接電波を受信する。CATV局105は衛星回線102より受信した放送電波をCATV回線106に中継し、CATV端末107はCATV回線106から放送電波を受信する。

【0088】図2は放送センタ101の内部構成の要部を示すブロック図の一例である。

【0089】放送センタ101は、映像や音声などを含むコンテンツを送出するコンテンツサーバ201と、第一のKw(ワーク鍵)を保持する第一のKw管理部203と、第二のKwを保持する第二のKw管理部206と、第一のKw及び直接受信端末104の契約情報を第一のEMM(個別情報)に格納し、直接受信端末装置固有のKm i

(個別鍵)で暗号化する第一のEMM生成部202と、一定間隔でKs(スクランブル鍵)を生成するKs生成部208と、Ks及び限定受信の対象となるコンテンツの視聴判定情報を第一のECMへ格納し、第一のKwを用いて暗号化する第一のECM生成部204と、Ks及び限定受信の対象となるコンテンツの視聴判定情報を第二のECMへ格納し、第二のKwを用いて暗号化する第二のECM生成部205と、Ksを第一のECM生成部204及び第二のECM生成部205へ送信し、Ks及びスクランブルの対象となるコンテンツのパケット識別子(PID)をスクランブラ210へ送信し、第一のECM生成部204及び第二のECM生成部205から入力する第一のECM及び第二のECMを多重部209へ送信するサイマルクリプト制御部207と、コンテンツ、第一のEMM、第一のECM及び第二のECMを多重してトランスポートストリームとして出力する多重部209と、トランスポートストリーム内のコンテンツのパケットをKsを用いてスクランブルするスクランブラ210と、衛星回線102に付いた変調などの処理を行う送信部211と、衛星回線102へトランスポートストリームを放送電波として送出する送信アンテナ212とを備えている。

【0090】コンテンツサーバ201はMPEG2規格のトランスポートストリーム形式で、映像や音声などを含むコンテンツを多重部209へ送信する。第一のKw管理部203は第一のKwを保持しており、第一のEMM生成部202及び第一のECM生成部204へ第一のKwを送信し、第一のEMM生成部202は第一のKw及び直接受信端末104の契約情報を第一のEMMに格納し、この直接受信端末装置固有のKm i(個別鍵)で、第一のEMM

の暗号化すべき領域を暗号化し、多重部209へ送信する。第二のKw管理部206は第二のKwを保持し、第二のECM生成部205へ第二のKwを送信し、Ks生成部208は一定間隔でKsを生成し、サイマルクリプト制御部207へ送信する。サイマルクリプト制御部207はKsを第一のECM生成部204及び第二のECM生成部205のそれぞれへ送信し、第一のECM生成部204は、Ks及び限定受信の対象となるコンテンツの視聴判定情報を第一のECMへ格納し、第一のKwを用いて、第一のECMの暗号化すべき領域を暗号化してサイマルクリプト制御部207へ送信する。第二のECM生成部205は、Ks及び限定受信の対象となるコンテンツの視聴判定情報を第二のECMへ格納し、第二のKwを用いて、第二のECMの暗号化すべき領域を暗号化してサイマルクリプト制御部207へ送信する。サイマルクリプト制御部207は、Ks及びスクランブルの対象となるコンテンツのパケット識別子(PID)をスクランブラ210へ送信し、第一のECM及び第二のECMを多重部209へ送信する。多重部209は、受信したコンテンツ、第一のEMM、第一のECM及び第二のECMを多重して1つのトランスポートストリームとしてスクランブラ210へ送信する。スクランブ

ラ210は、サイマルクリプト制御部207から受信したP I Dを基に、トランスポートストリーム内の該当するコンテンツのバケットをK sを用いてスクランブルを行い、送信部211へ送信する。送信部211は衛星回線102に於いた変調などの処理を行い、送信アンテナ212を介して、衛星回線102へトランスポートストリームを放送電波として送出する。

【0091】図3はCATV局105の内部構成の要部を示すブロック図の一例である。

【0092】CATV局105は、衛星回線102から放送電波を受信する受信アンテナ301と、受信信号の復調などの処理を行う受信部302と、N I Tを衛星伝送用途からケーブル伝送用途に変換するP S I変換部303と、放送センタ101の第二のK w管理部206と同一の第二のK wを保持している第二のK w管理部307と、第二のK w及びCATV端末107の固有のK m iで暗号化する第二のECM生成部308と、P S I変換部303から入力するトランスポートストリームに第二のECMを多重して1つのトランスポートストリームにする多重部304と、トランスポートストリームにCATV回線106に於いた変調を行うQAM変調部305と、トランスポートストリームを伝送すべき周波数帯へ変換する周波数変換部306と、トランスポートストリームをCATV回線106へ送出する混合部309とを備えている。

【0093】受信部302は衛星回線102から受信アンテナ301を介して放送電波を受信し、復調などの処理を行い、中継すべきトランスポートストリームをP S I変換部303へ送信する。P S I変換部303は、番組配列情報(P S I)の一部であり、変調周波数などの伝送路の情報とコンテンツとを関連付ける情報を伝送するためのN I T(Network_Information_Table)を、衛星伝送用途からケーブル伝送用途に変換して多重部304へ送信する。第二のK w管理部307は放送センタ101における第二のK w管理部206と同一の第二のK wを保持しており、第二のECM生成部308へ第二のK wを送信する。第二のECM生成部308は、第二のK w及びCATV端末107の固有のK m iで、第二のECMの暗号化すべき領域を暗号化し、多重部304へ送信する。多重部304はトランスポートストリームに更に第二のECMを多重して1つのトランスポートストリームにしてQAM変調部305へ送信し、QAM変調部305はトランスポートストリームにCATV回線106に於いた変調を行い周波数変換部306へ送信し、周波数変換部306はトランスポートストリームを伝送すべき周波数帯へ変換して混合部309へ送信し、混合部309は、必要な情報を混合(この場合には混合すべき情報は特に無い)したトランスポートストリームをCATV回線106へ送出する。

【0094】図4は直接受信端末104の内部構成の要部を示すブロック図の一例である。

【0095】直接受信端末104は、衛星回線102から受信アンテナ401を介して選択した放送電波を受信するチューナ402と、受信したトランスポートストリームに復調処理を行う復調部403と、トランスポートストリームから第一のECM及び第一のECMとその他とを分離する分離部404と、第一のECMを復号して契約情報及び第一のK wを抽出し、第一のECMを第一のK wで復号して視聴判定情報及びK sを抽出する限定受信モジュール405と、抽出されたK sを用いてトランスポートストリーム内のコンテンツのバケットをデスクランブルするデスクランブラ406と、コンテンツを出力形態に応じた信号に変換する出力制御部407とを備えている。

【0096】この直接受信端末104のチューナ402は、衛星回線102から受信アンテナ401を介して放送電波を受信し、受信すべきトランスポートストリームを復調部403へ送信する。復調部403はトランスポートストリームに、放送センタ101における送信部211に於いた変調処理を行い、分離部404へ送信し、分離部404はトランスポートストリームから第一のECM及び第一のECMを分離して限定受信モジュール405へ送信し、残りのトランスポートストリームをデスクランブラ406へ送信する。限定受信モジュール405は、第一のECMを予め保持しているK m iを用いて復号し、契約情報及び第一のK wを抽出保持し、第一のECMを受信したときに第一のK wを用いて復号し、視聴判定情報及びK sを抽出し、契約情報と視聴判定情報とを比較して、視聴可能と判定した場合にK sをデスクランブラ406へ送信する。デスクランブラ406はK sを用いてトランスポートストリーム内のコンテンツのバケットをデスクランブルして、出力制御部407へ送信し、出力制御部407はコンテンツを出力形態に応じた信号に変換するなどの処理、例えば、テレビに出力する場合にはテレビ信号への変換など、を行い送出する。

【0097】図5はCATV端末107の内部構成の要部を示すブロック図の一例である。

【0098】CATV端末107は、CATV回線106から放送信号を受信するチューナ502と、受信したトランスポートストリームに復調処理を行う復調部503と、トランスポートストリームから第二のECM及び第二のECMとその他とを分離する分離部504と、第二のECMを復号して契約情報及び第二のK wを抽出し、第二のECMを第二のK wで復号して視聴判定情報及びK sを抽出する限定受信モジュール505と、抽出されたK sを用いてトランスポートストリーム内のコンテンツのバケットをデスクランブルするデスクランブラ506と、コンテンツを出力形態に応じた信号に変換する出力制御部507とを備えている。

【0099】このCATV端末107のチューナ502は、C

ATV回線106から放送信号を受信し、受信すべきトランスポートストリームを復調部503へ送信する。復調部503はトランスポートストリームに、CATV局105におけるQAM変調部305に於いた復調処理を行い、分離部504へ送信し、分離部504はトランスポートストリームから第二のECM及び第二のECMを分離して限定受信モジュール505へ送信し、残りのトランスポートストリームをデスクランブラ506へ送信する。限定受信モジュール506は、第二のECMを予め保持しているK m iを用いて復号し、契約情報及び第二のK wを抽出保持し、第二のECMを受信したときに第二のK wを用いて復号し、視聴判定情報及びK sを抽出し、契約情報と視聴判定情報とを比較して、視聴可能と判定した場合にK sをデスクランブラ506へ送信する。デスクランブラ506はK sを用いてトランスポートストリーム内のコンテンツのバケットをデスクランブルし、出力制御部507へ送信し、出力制御部507はコンテンツを出力形態に応じた信号に変換するなどの処理、例えば、テレビに出力する場合にはテレビ信号への変換など、を行い送出する。

【0100】以上の構成よりなる限定受信システムにおいて、以下その動作を説明する。

【0101】放送センタ101において、コンテンツサーバ201は1つ以上のコンテンツを送出するものとし、このコンテンツはMPEG2のトランスポートストリーム形式であり、コンテンツに含まれる音声や映像などは全てバケット形式で伝送され、さらに、1つ以上のコンテンツが1つのトランスポートストリーム内に含まれ、それぞれのコンテンツをチャンネルとして表現する。このチャンネルの構成、つまり、それぞれのコンテンツに含まれるバケットの構成などを表すためのP S I(番組配列情報)もコンテンツサーバ201が送出するものとする。

【0102】第一のK w管理部203は、第一のK w及びベアとなるK w I Dを第一のECM生成部202及び第一のECM生成部204に送信する。

【0103】第一のECM生成部202は各直接受信端末104に対して第一のECMを送出する。ECMの基本構成は図6に示すように、端末I D601、K w I D602、K w格納領域603及び契約情報領域604を含む。この基本構成は第一のECM及び(CATV局で生成される)第二のECMに共通であり、第一のECMについて説明すると、端末I D601はECMの宛先となる直接受信端末104固有の端末I D(識別番号)を格納し、K w I D602には第一のK wを変更する際などに2つ以上の第一のK wが必要となる場合にそれぞれの第一のK wを識別するためのK w I D(ワーク識別)を格納し、K w格納領域603にはK w I D602に格納したK w I Dとベアとなる第一のK wそのものを格納し、契約情報領域604には端末I D602に格納した端末I Dに該当する直接受信端末104の契約情報を格納する。また、K w I D602、K w格

納領域603及び契約情報領域604は端末I Dに該当する直接受信端末104固有のK m i(個別鍵)で暗号化する。第一のECM生成部202はこのような第一のECMを生成して送出する。

【0104】サイマルクリプト制御部207は、K s生成部208から受信したK sを第一のECM生成部204及び第二のECM生成部205に送信する。

【0105】第一のECM生成部204はコンテンツに付随する第一のECMを生成して送出する。ECMの基本構成は図7に示すように、K w I D701、K s格納領域702、視聴判定領域703を含む。この基本構成は第一のECM及び第二のECMに共通であり、第一のECMについて説明すると、K w I D701は第一のECMを暗号化する第一のK wの識別子であり、第一のECM内のK w I D602に相当する。K s格納領域702はコンテンツをスクランブルするK sを格納し、視聴判定領域703はコンテンツの視聴判定を行うための情報を格納する。また、K s格納領域702及び視聴判定領域703をK w I D701に格納したK w I Dとベアとなる第一のK wを用いて暗号化する。第一のECM生成部204はこのような第一のECMを生成してサイマルクリプト制御部207へ送信する。

【0106】第二のK w管理部206は、第二のECM生成部205に対して第二のK w及びベアとなるK w I Dを送信する。

【0107】第二のECM生成部205は、コンテンツに付随する第二のECMを生成して送出する。図7のECM基本構成をもとに、第二のECMについて説明すると、K w I D701は第二のK wの識別子であり、第二のECM内のK w I D602に相当し、第一のECMに格納したK w I Dと同一である必要はない。K s格納領域702はコンテンツをスクランブルするK sを格納し、この場合、第一のECMに格納したK sと同一のK sを格納する。視聴判定領域703はコンテンツの視聴判定を行うための情報を格納し、この場合は第一のECMに格納した視聴判定情報と同一である必要はない。また、K s格納領域702及び視聴判定領域703をK w I D701に格納したK w I Dとベアとなる第二のK wを用いて暗号化する。第二のECM生成部205はこのような第二のECMを生成してサイマルクリプト制御部207へ送信する。

【0108】サイマルクリプト制御部207は、スクランブルを行う対象となるコンテンツのバケット識別(P I D)とK sとをスクランブラ210へ送信し、第一のECM及び第二のECMを多重部209へ送信する。

【0109】多重部209はコンテンツ、第一のECM、第一のECM及び第二のECMを多重して1つのトランスポートストリームにして送信し、スクランブラ210は指定されたP I Dをもとに、トランスポートストリーム内でスクランブルの対象となるコンテンツのバケットをスクランブルして送信し、送信部211、送信アンテナ212

を介して放送電波として衛星回線102へ送出する。

【0110】CATV局105において、PSI変換部303は受信したトランスポートストリーム内のNITを書き換えるが、具体的には、受信したNITには衛星回線102からの放送電波を受信した際の物理情報などが記述されており、この情報をもとに放送電波から適切なトランスポートストリームを受信することが可能となっている。このNITをそのままCATV回線106へ中継しては、CATV端末107でトランスポートストリームを受信することができなくなるので、NITを衛星回線102に送った内容からCATV回線106に送った内容に変更する。

【0111】CATV局109内の第二のKw管理部307は、放送センタ101内の第二のKw管理部206と同一の第二のKwを管理しており、KwIDと第二のKwとを第二のEMM生成部308へ送信する。

【0112】第二のEMM生成部308は、各CATV端末107に対して第二のEMMを送出する。第二のEMMについて図8を用いて説明すると、端末ID601には第二のEMMの宛先となる各CATV端末107固有の端末IDを格納し、KwID602には第二のKwを変更する際に2つ以上の第二のKwが必要となる場合にそれぞれの第二のKwを識別するためのKwIDを格納し、Kw格納領域603にはKwID602に格納したKwIDとペアとなる第二のKwそのものを格納し、契約情報領域604には端末ID601に格納した端末IDに該当するCATV局107の契約情報を格納する。また、KwID602、Kw格納領域603及び契約情報領域604は端末ID601に該当するCATV局107固有のKwIDで暗号化する。第二のEMM生成部308はこのような第二のEMMを生成して多重部304へ送出する。

【0113】多重部304は、トランスポートストリームにさらに第二のEMMを多重して1つのトランスポートストリームにして送出し、QAM変調部305、周波数変換部306、混合部309を介してCATV回線106へ放送信号として送出する。

【0114】直接受信端末104において、受信アンテナ401、チューナ402及び復調部403を介して衛星回線102から視聴したいコンテンツを含むトランスポートストリームを受信し、分插部404はトランスポートストリームから第一のECM及び自分宛の第一のEMMを分離して限定受信モジュール405へ送信する。

【0115】限定受信モジュール405は、第一のEMMの契約情報と第一のECMの視聴判定情報とを比較して視聴可能と判定した場合にKsをデスクランブラ405へ送信する。

【0116】図8に示すフローチャートは基本的な視聴判定処理を示し、限定受信モジュール405及びCATV局105の限定受信モジュール505の基本処理であり、まず、限定受信モジュール405について説明する。

【0117】第一のEMMは契約した時点で、予め受信しており、これをKmiを用いて復号し、KwID、第一のKw及び契約情報を保持しておく。

【0118】ステップ801: 第一のECMを受信し非暗号部のKwIDをもとに、該当する第一のKwを用いて暗号部の復号を行う。

【0119】ステップ802: 復号された視聴判定情報と予め保持している契約情報とを比較して視聴可能と判定すれば、

ステップ803: Ksをデスクランブラ406へ送信する。

【0120】ステップ802において、視聴不可能と判定すれば、

ステップ804: エラー処理、例えば、契約されていない旨を返信するなどを行う。

【0121】ステップ802における判定方法がティア判定であるとなると、第一のEMMの契約情報領域には契約情報を示すティアビットを記述し、第一のECMの視聴判定領域にはコンテンツの視聴判定を示すティアビットを記述する。視聴判定領域をティアビットで記述した場合は図9のような構成になっており、また、契約情報領域をティアビットで記述した場合には図10のような構成になっている。例えば、プロ野球及び阪神戦に属する全てのコンテンツに付随する第一のECMの視聴判定ティアビット901は、図9のように、該当するビットが1になっており、また、映画シリーズA及び阪神戦を契約した第一のEMMの契約情報ティアビット1001は、図10のように、該当するビットが1になっている。そして、契約情報ティアビット1001をもつ第一の端末装置104が、視聴判定ティアビット901をもつ第一のECMに付随するコンテンツを視聴しようとする場合、視聴判定ティアビット901と契約情報ティアビット1001とのビット比較を行い、1つの項目だけでもそれぞれが1である項目があれば視聴可能となる。つまり、この例では阪神戦の項目がお互いに1であるので、視聴可能となる。逆に、契約情報1001をもつ第一の端末装置104がプロ野球及び巨人戦に属するコンテンツを視聴しようとした場合には、そのコンテンツの視聴判定ティアビットはプロ野球及び巨人戦の項目だけが1であるので、ビット比較を行っても、お互いが1になる項目が1つもないので、視聴することができない。また、プロ野球を契約した場合は契約情報ティアビットはプロ野球の項目が1になるので、上記のプロ野球及び阪神戦に属するコンテンツ、並びに、プロ野球及び巨人戦に属するコンテンツは両方視聴可能となる。このようにティアビットで表す場合はティアビットの1つの項目に複数のコンテンツが含まれることもあり、1つのコンテンツが複数の項目に属することもある。

【0122】CATV局107において、チューナ502及び復調部503を介してCATV回線106から視聴したいコンテンツを含むトランスポートストリームを受信し、分

離部504はトランスポートストリームから第二のECM及び自分宛の第二のEMMを分離して限定受信モジュール505へ送信する。

【0123】限定受信モジュール505は、第二のEMMの契約情報と第一のECMの視聴判定情報とを比較して視聴可能と判定した場合にKsをデスクランブラ506へ送信する。具体的には上記に示した図8のフローチャートと同様の判定処理であり、第二のEMMは予め受信しており、Kmiを用いて復号し、KwID、第二のKw及び契約情報を保持しておく。ステップ802にて、第二のECMを受信し非暗号部のKwIDをもとに、該当する第二のKwを用いて暗号部の復号を行う。ステップ803へ移行し、Ksをデスクランブラ506へ送信し、視聴不可能と判定すればステップ804へ移行し、エラー処理、例えば、契約されていない旨を返信するなどを行う。ステップ802における判定方法はチャンネルビットマップであるとなると、第二のEMMの契約情報領域には契約情報を示すビットマップを記述し、第二のECMの視聴判定領域にはコンテンツの視聴判定を示すビットマップを記述する。視聴判定領域をビットマップで記述した場合は図11のような構成になっており、また、契約情報領域をビットマップで記述した場合は図12のような構成になっている。例えばチャンネル3(CH3)のコンテンツの視聴判定ビットマップ1101は図11のように該当する項目のみが1となっており、また、CH2、CH3、CHNを契約した場合の契約情報ビットマップ1201は図12のように該当する項目が1になっている。そして、契約情報ビットマップ1201をもつCATV局107が視聴判定ビットマップ1101をもつ第二のECMに付随するコンテンツを視聴しようとする場合、ビット比較を行い、1つの項目だけでもそれぞれが1である項目があれば視聴可能となる。つまり、この例ではCH3の項目がお互いに1であるので、視聴可能となる。逆に契約情報ビットマップ1201をもつCATV局107がCH1を視聴しようとした場合には、CH1のコンテンツの視聴判定ビットマップはCH1のみが1であるので、ビット比較を行っても、お互いが1になる項目がなく、視聴することができない。このようにビットマップで表す場合にはビットマップの1つの項目が1つのチャンネルに相当する。

【0124】以上のように、本実施の形態によれば、放送センタ101がコンテンツとともに第一のECM、第二のECM及び第一のEMMを送出し、CATV局105が第一のECM及び第一のEMMを用いてコンテンツに対する視聴判定を行い、CATV局107が第二のECM及び第二のEMMを用いてコンテンツに対する視聴判定を行うようにしたので、放送センタ101が直接受信端末104

の限定受信を管理し、CATV局105が独立してCATV局105の限定受信を管理することができるという効果が得られる。また、CATV局105はコンテンツを含む情報を中継する際に、コンテンツのデスクランブルや、第一のECM、第二のECM、第一のEMMの復号を行う必要がないので、簡単な構成で中継することが可能となり、設備の低コスト化が図れる。また、直接受信端末104の視聴判定をティアビットとし、CATV局107の視聴判定をビットマップとできるので、CATV局105はより独立して運用を行うことが可能となる。

【0125】なお、本実施の形態において、第一のECM生成部204と第二のECM生成部205の行暗号化方式を別々のものとすれば、いずれかの暗号化方式が破られたとしても、もう片方は影響なく運用できるので、CATV局105はより独立して限定受信の運用を行うことが可能となる。

【0126】また、第一のEMM生成部202と第二のEMM生成部308の行暗号化方式を別々のものとすれば、いずれかの暗号化方式が破られたとしても、もう片方は影響なく運用できるので、CATV局105はより独立して限定受信の運用を行うことが可能となる。

【0127】また、図8に示したEMMの基本構成図は、あくまでも基本であり、第一のEMM及び第二のEMMが同じフォーマットである必要はなく、別々のフォーマットで実現することも可能であり、この場合には、CATV局105はより独立して限定受信の運用を行うことが可能となる。

【0128】また、図7に示したECMの基本構成図も同様、あくまでも基本であり、第一のECM及び第二のECMが同じフォーマットである必要はなく、別々のフォーマットで実現することが可能であり、この場合には、CATV局105はより独立して限定受信の運用を行うことが可能となる。

【0129】また、本実施の形態では、直接受信端末104の視聴判定をティアビットとし、CATV局107の視聴判定をビットマップとしたが、それぞれの視聴判定は逆の方法でもよく、また、いずれか一方の方法でもよく、さらには、ティアビットとビットマップとを組み合わせたことも可能であり、様々な運用が可能となる。また、限定受信モジュール405及び505は、内蔵のチップなどでもよいし、取り外し可能なICカードやPCMCIAカードなどでもよい。

【0130】なお、放送センタ101内の第二のKw管理部206と、CATV局109内の第二のKw管理部307とが同一の第二のKwを共有する方法としては、第二のKw管理部206がフロッピーやICカードなどの記憶媒体に第二のKwを書き込み、CATV局105に送り、第二のKw管理部307が記憶媒体から読み出すことで、第二のKwの共有化が可能となる。また、逆に、CATV局105の第二のKw管理部307が第二のKwを記憶媒体に書き

の限定受信を管理し、CATV局105が独立してCATV局105の限定受信を管理することができるという効果が得られる。また、CATV局105はコンテンツを含む情報を中継する際に、コンテンツのデスクランブルや、第一のECM、第二のECM、第一のEMMの復号を行う必要がないので、簡単な構成で中継することが可能となり、設備の低コスト化が図れる。また、直接受信端末104の視聴判定をティアビットとし、CATV局107の視聴判定をビットマップとできるので、CATV局105はより独立して運用を行うことが可能となる。

【0125】なお、本実施の形態において、第一のECM生成部204と第二のECM生成部205の行暗号化方式を別々のものとすれば、いずれかの暗号化方式が破られたとしても、もう片方は影響なく運用できるので、CATV局105はより独立して限定受信の運用を行うことが可能となる。

【0126】また、第一のEMM生成部202と第二のEMM生成部308の行暗号化方式を別々のものとすれば、いずれかの暗号化方式が破られたとしても、もう片方は影響なく運用できるので、CATV局105はより独立して限定受信の運用を行うことが可能となる。

【0127】また、図8に示したEMMの基本構成図は、あくまでも基本であり、第一のEMM及び第二のEMMが同じフォーマットである必要はなく、別々のフォーマットで実現することも可能であり、この場合には、CATV局105はより独立して限定受信の運用を行うことが可能となる。

【0128】また、図7に示したECMの基本構成図も同様、あくまでも基本であり、第一のECM及び第二のECMが同じフォーマットである必要はなく、別々のフォーマットで実現することが可能であり、この場合には、CATV局105はより独立して限定受信の運用を行うことが可能となる。

【0129】また、本実施の形態では、直接受信端末104の視聴判定をティアビットとし、CATV局107の視聴判定をビットマップとしたが、それぞれの視聴判定は逆の方法でもよく、また、いずれか一方の方法でもよく、さらには、ティアビットとビットマップとを組み合わせたことも可能であり、様々な運用が可能となる。また、限定受信モジュール405及び505は、内蔵のチップなどでもよいし、取り外し可能なICカードやPCMCIAカードなどでもよい。

【0130】なお、放送センタ101内の第二のKw管理部206と、CATV局109内の第二のKw管理部307とが同一の第二のKwを共有する方法としては、第二のKw管理部206がフロッピーやICカードなどの記憶媒体に第二のKwを書き込み、CATV局105に送り、第二のKw管理部307が記憶媒体から読み出すことで、第二のKwの共有化が可能となる。また、逆に、CATV局105の第二のKw管理部307が第二のKwを記憶媒体に書き

込み、放送センタ101に送り、第二のKw管理部206が記憶媒体を読み出すようにしても良い。また、この場合に、複数のCATV局105が放送センタ101に接続されている場合には、ある1つのCATV局105から記憶媒体を放送センタ101に送り、放送センタ101がその他のCATV局105へ送る方法もある。また、ある1つのCATV局105から放送センタ101及びその他のCATV局105へ、記憶媒体を送る方法もある。

【0131】また、第二のKwの共有方法の別の方法としては、放送センタ101において、第二のKw管理部206が送信部211に接続されているとして、送信部211及び送信アンテナ212を介して衛星回路102へ第二のKwを送信し、CATV局105では第二のKw管理部307が受信部302へ接続されているものとして、受信アンテナ301及び受信部302を介して第二のKwを受信する方法もある。また、送信アンテナ212、受信アンテナ301及び衛星回路102が双方向通信可能であるとして、CATV局105の第二のKw管理部307から衛星回路102へ第二のKwを送信し、放送センタ101の第二のKw管理部206が衛星回路102を介して第二のKwを受信する方法もある。また、この場合に、複数のCATV局105が放送センタ101に接続されている場合には、ある1つのCATV局105から放送センタ101へ衛星回路102を介して第二のKwを送信し、放送センタ101がその他のCATV局105へ衛星回路102を介して送信する方法もある。また、ある1つのCATV局105から放送センタ101及びその他のCATV局105へ衛星回路102を介して送信する方法もある。この衛星回路102を利用する場合には、第二のKwをCATV局105宛のEMMに格納して送達するようにしてもよい。

【0132】また、第二のKwの共有方法の別の方法としては、放送センタ101の第二のKw管理部206と、CATV局105の第二のKw管理部307とが公衆網で接続されているとして、公衆網を介して共有する方法がある。この方法も上記2つの方法と同様に、放送センタ101からCATV局105へ送信する方法と、ある1つのCATV局105から放送センタ101へ送信し、放送センタ101がその他のCATV局105へ送信する方法と、ある1つのCATV局105から放送センタ101及びその他のCATV局105へ送信する方法とがある。

【0133】また、第二のKwを記憶媒体や衛星回路102及び公衆網を用いて送達する場合に、秘密鍵暗号方式や公開鍵暗号方式を利用して第二のKwに暗号を施すことで、秘匿性を向上させることが可能となる。

【0134】(第2の実施の形態) 図13はCATV局105における多重部304の要部の構成を示す一例である。

【0135】多重部304は、共通情報除去装置1301及び多重装置1302を含む。共通情報除去装置1301は、PSI変換部303からトランスポートストリームを受信して第一のECMを除去し、多重装置1302は、この第一のEC

Mが除去されたトランスポートストリームに第二のECMを多重してQAM変調部305へ送信する。放送センタ101やCATV局105のその他の構成や直接受信端末104及びCATV端末107の構成は第1の実施の形態と同様であるので、流用して以下、動作を説明する。

【0136】共通情報除去装置1301がトランスポートストリームから第一のECMを除去する方法としては、第一のECMや第二のECMなどは全てMPEG2トランスポートストリームのパケット形式であるので、図14に示すようにパケットの種類を識別するための番号であるPID(パケット識別子)がTSパケットヘッダ1401に付与されている。よって、第一のECMと第二のECMのPIDを別々の値にすれば簡単に除去することが可能である。

【0137】また、別の除去方法としては、第一のECMと第二のECMのPIDが同じ値の場合に、図15に示すようにECMの非暗号部にECM識別子1501を設け、ECM識別子1501の値を第一のECMと第二のECMとで別々の値とすればECMを番号せずに簡単に除去することが可能となる。

【0138】以上のように、本実施の形態によれば、共通情報除去装置1301が第一のECMを除去するようにしたので、CATV端末107には必要のない情報が流されることがなく、CATV端末107の誤動作防止につながる。さらに、CATV回路106上で、第一のECM以外の伝送容量を増加させることができるという効果が得られる。

【0139】なお、映像や音声などには再生するための時間情報が含まれているが、共通情報除去装置1301が、第一のECMを除去した際に、その差分を時間情報に反映させて再計算することも、必要に応じて行ってもよく、このようにすればコンテンツの再生に影響を及ぼさずに除去できる。

【0140】また、共通情報除去装置1301は第一のECMを除去するのではなく、空の情報(ヌルパケット)と入れ替えてもよく、この場合は、CATV端末107の誤動作防止につながる。

【0141】(第3の実施の形態) 図16はCATV局105における多重部304の要部の構成を示す一例である。

【0142】多重部304は、個別情報除去装置1601及び多重装置1602を含む。個別情報除去装置1601は、PSI変換部303からトランスポートストリームを受信し、第一のEMMを除去して、多重装置1602へ送信し、多重装置1602は、トランスポートストリームに第二のEMMを多重してQAM変調部305へ送信する。その他の構成は第1の実施の形態と同様であるので、流用して以下、動作を説明する。

【0143】個別情報除去装置1601がトランスポートストリームから第一のEMMを除去する方法としては、第一のEMMや第二のEMMはMPEG2トランスポート

ストリームのパケット形式であるので、そのPIDを別々の値にすれば簡単に除去することが可能である。

【0144】また、別の除去方法としては、第一のEMMと第二のEMMのPIDが同じ値の場合に、図17に示すようにECMの非暗号部にECM識別子1701を設け、ECM識別子1701の値を第一のEMMと第二のEMMとで別々の値とすればECMを番号せずに簡単に除去することが可能となる。

【0145】図18は多重装置1602の動作を説明する図である。多重装置1602は、1パケット以上のバッファを有しており、トランスポートストリームをバッファに蓄えながらパケットの種類をチェックし順次送出していく。また、第二のEMM生成部308から受信した第二のEMMを保持するバッファも1パケット以上有している。そして、第二のEMMを保持している場合、トランスポートストリーム内にヌルパケット(空の情報)を検出すると、保持している第二のEMMとヌルパケットとを入れ替えて送信する。

【0146】以上のように、本実施の形態によれば、個別情報除去装置1601が第一のEMMを除去するようにしたので、CATV端末107には必要のない情報が流されることがなく、CATV端末107の誤動作防止につながる。さらに、CATV回路106上で、第一のEMM以外の伝送容量を増加させることができるという効果が得られる。

【0147】また、多重装置1602が第二のEMMをヌルパケットと入れ替えて送信するようにしたので、多重装置1602はトランスポートストリームの伝送速度を変更することなく第二のEMMを多重することが可能となり、CATV端末107に必要のない第一のEMMを削除することも可能であるので、CATV端末107の誤動作を防止することができるという効果が得られる。

【0148】なお、映像や音声などには再生するための時間情報が含まれているが、個別情報除去装置1601が、第一のEMMを除去した際に、その差分を時間情報に反映させて再計算することも、必要に応じて行ってもよく、このようにすればコンテンツの再生に影響を及ぼさずに除去できる。

【0149】また、多重装置1602がトランスポートストリームを保持する時間を、再生のための時間情報に反映させて再計算することも、必要に応じて行うようにすればコンテンツの再生に影響を及ぼすことはない。

【0150】また、個別情報除去装置1601は、第一のEMMを除去するのではなく、ヌルパケットと入れ替えてもよく、この場合はCATV端末107の誤動作防止につながる。

【0151】また、多重装置1602は、第二のEMMをヌルパケットと入れ替えて送信するとしても、ヌルパケットだけではなく、第一のECMと入れ替えて送信することも可能であり、このようにすれば、トランスポートストリームの伝送速度を変更すること無しに、第二のEMMの伝送容量を増加させることが可能になるという効果が得られる。

【0152】(第4の実施の形態) 図19はCATV局105における多重部304の要部の構成を示す一例である。

【0153】多重部304は個別情報多重装置1901を含み、個別情報多重装置1901はPSI変換部303からトランスポートストリームを受信し、また、第二のEMM生成部308から第二のEMMを受信し、トランスポートストリーム内の第一のEMMと第二のEMMとを入れ替えて送信する。その他の構成は第1の実施の形態と同様であるので、流用して以下、動作を説明する。

【0154】図20は個別情報多重装置1901の動作を説明する図である。個別情報多重装置1901は1パケット以上のバッファを有しており、トランスポートストリームをバッファに蓄えながらパケットの種類をチェックし順次送出していく。また、第二のEMM生成部308から受信した第二のEMMを保持するバッファも1パケット以上有している。そして、第二のEMMを保持している場合、トランスポートストリーム内に第一のEMMを検出すると、保持している第二のEMMと第一のEMMとを入れ替えて送信する。また、第二のEMMを保持していない場合には第一のEMMをヌルパケットに置き換えることで、CATV端末107に必要のない情報を削除することができる。

【0155】以上のように、本実施の形態によれば、個別情報多重装置1901が、第一のEMMに替えて、第二のEMMまたはヌルパケットを送信するようにしたので、個別情報多重装置1901はトランスポートストリームの伝送速度を変更することなく第二のEMMを多重することが可能となり、CATV端末107に必要のない第一のEMMを削除することも可能であるので、CATV端末107の誤動作を防止することができるという効果が得られる。

【0156】なお、本実施の形態では、個別情報多重装置1901が第二のEMMを第一のEMMと入れ替えるとしたが、第二のEMMをヌルパケットや第一のECMと入れ替えてもよく、このようにすれば、トランスポートストリームの伝送速度を変更することなく第二のEMMの伝送容量を増やすことができる。さらに、この場合、第二のEMMを保持していないときは、第一のECMはヌルパケットと置き換えるようにしてもよく、CATV

端末107の誤動作防止につながる。

【0157】また、必要に応じて映像や音声の再生のための時間情報を再計算するようにしてもよい。

【0158】(第5の実施の形態) 図21はCATV局105における多重部304の要部の構成を示す一例である。

【0159】多重部304は共通情報多重装置2101及び多重装置2102を含む。共通情報多重装置2101はPSI変換部303からトランスポートストリームを受信し、第二のECMを受信すると、それを、次の第二のECMを受信するまで、一定間隔で繰り返し多量装置2102へ送信する。多重装置2102は、トランスポートストリームに、こ

の第二のECMを多重して送信する。その他の構成は第1の実施の形態と同様であるので、流用して以下、動作を説明する。

【0180】図22は共通情報多重装置210における、第二のECMの受信タイミングと送信タイミングを示す図である。

【0181】通常、放送センタ10はKs（スクランブル）を一定間隔で更新し、そのたびに第一のECMを変更し、送出する。直接受信端末104がKsを正常に受信しなくてはコンテンツの視聴ができなくなるので、Ks更新間隔を3秒として、第一のECM送信間隔は500ミリ秒にするなどというように、第一のECM送信間隔はKs更新間隔よりも短く設定されている。

【0182】同様に、CATV端末107についてもKsを正常に受信する必要があるため、第二のECMをKs更新間隔の間に数回行う必要がある。そこで、図22に示すように、放送センタ10からはKsの更新、つまり第二のECM更新のたびに1度送信し、共通情報多重装置210が次の第二のECMを受信するまで第二のECMの再送を行う。このようにすれば、放送センタ10が第二のECMを再送する場合に比べて、衛星回線102上の、第二のECM以外の情報の伝送容量を増加でき、CATV端末107もKsを正常に受信できるという効果が得られる。

【0183】なお、第二のECMを再送する際には、図14に示したTSパケットヘッダ1401の巡回カウンタを順次更新する。

【0184】また、第二のECMの再送処理の終了の方法としては、上記の一定間隔よりも長い期間内に次の第二のECMを受信しない場合に終了するという方法がある。別の方法としては、第二のECMの非符号部の領域に最後のECMであることを示す識別子を設ける方法もある。また、別の方法としては、対応する映像や音声などのTSパケットヘッダ1401のスクランブル制御を示す項目をチェックし、スクランブルされていないと判断した場合に、該当の第二のECMの送出を終了するという方法もある。

【0185】以上のように、本実施の形態によれば、放送センタ10は第二のECMを更新のたびに1度だけ送信し、CATV局105の共通情報多重装置210が第二のECMの再送処理を行うようにしたので、衛星回線102において第二のECM以外の情報の伝送容量を増加できるという効果が得られる。

【0186】なお、共通情報多重装置210が第二のECMを再送する場合には、第一のECMや第一のECM、またはMLパケットと入れ替えて送信するようにしても良い。

【0187】また、図23は第二のECMのフォーマッ

トの要部を示す図である。

【0188】図23に示すように、第二のECMの非符号部に、CATV端末107で行う視聴判定をティア判定か、PPV（ペイパービュー）判定にするかを示す番組属性2301を設け、放送センタ10からは視聴判定領域にティア情報2304及びPPV（ペイパービュー）情報2305を格納し、番組属性2301には判定方法を指定せずに送出する。共通情報多重装置210は第二のECMを受信すると、対応するコンテンツの運用方法に応じて、番組属性2301をティア判定、PPV判定のいずれか、または、両方を示す値に変更して送出する。

【0189】CATV端末107は番組属性2301をチェックし、ティア判定であれば、契約情報ティアビットと第二のECMのティア情報2304とを比較して視聴判定を行い、また、PPV判定であれば、PPVの契約情報とPPV情報2305とを比較して視聴判定を行う。番組属性2301が、ティア判定及びPPV判定の両方を示している場合には、いずれかの視聴判定において視聴可能と判定すれば視聴が可能となる。

【0190】このように、第二のECMに番組属性2301を設け、放送センタ10は第二のECMにティア情報2304及びPPV情報2305を格納して送出し、共通情報多重装置210が運用に応じて番組属性2301を変更するようにしたので、CATV局105はより独立して柔軟な運用ができるという効果が得られる。

【0191】また、複数のCATV局105が放送センタ10に接続されている場合、あるCATV局105ではあるコンテンツをティアで運用して、別のCATV局105では同一のコンテンツをPPVで運用できる。このように、柔軟な運用ができる効果が得られる。

【0192】（第8の実施の形態）図24は第二のECMのフォーマットの要部を示す図である。システム構成は第5の実施の形態と同じであるので、流用して以下動作を説明する。

【0193】図24に示すように、放送センタ10からは、第二のECMにKs 2402、及び暗号部を符号化した第二のKwのKwID 2401を格納して送出する。CATV局105では図21に示す共通情報多重装置210がCATV局105独自の視聴判定領域2403を追加して第二のECMを送信する。

【0194】以上のように、本実施の形態によれば、共通情報多重装置210が第二のECMにCATV局105独自の視聴判定領域2403を追加して送信するようにしたので、CATV局105はより独立して限定受信の制御が可能となる。

【0195】また、図25は共通情報多重装置210が第二のECMを送信する際の、上記とは別の例であるフォーマットの要部を示す図である。図26はCATV端末107へ送信する第二のECMのフォーマットの要部を示す図である。

【0176】図25に示すように、共通情報多重装置210は第二のECMに、視聴判定領域2403を追加して、第二のKwのKwID 2401、Ks 2402及び視聴判定領域2403を含む領域を第三のKwを用いて暗号化し、さらに第三のKwのKwID 2501を第二のECMに追加して送信する。このようにすれば、視聴判定領域2403の秘匿性を確保することができる。

【0177】このとき、CATV端末107に第三のKwを通知する必要があるが、CATV局105の第二のECM生成部308から図26に示すように、第二のECMに第三のKw 2605及び対応する第三のKwのKwID 2604を格納して送信する。CATV端末107はこれより第三のKwを知ることができるので、図25に示す第二のECMを復号することができ、限定受信が可能となる。

【0178】以上のようにすれば、CATV局105はより独立して限定受信の制御が可能となり、視聴判定領域2403の秘匿性も確保できるという効果が得られる。

【0179】（第7の実施の形態）図27はCATV局105の内部構成の要部を示す図の一例である。

【0180】このCATV局105は、第二のECM生成部2707で生成した第二のECMを、多重部を通じてストリームに多重する代わりに、第二のECMを変調する変調部2710と、それを周波数変換する周波数変換部2708とを備え、第二のECMを変調、周波数変換した後、混合部2709でストリームと混合している。

【0181】このCATV局105では、受信部2702が衛星回線102から中継するストリームを受信し、PSI変換部2703へ送信し、PSI変換部2703では第1の実施の形態と同様に、NITをCATV回線106に送った内容に変更してQAM変調部2704へ送信し、QAM変調部2704はCATV回線106に送った変調を行い、周波数変換部2705へ送信し、周波数変換部2705はコンテンツを含むストリームをCATV回線106上の対応する周波数帯域に変換して混合部2709へ送信する。

【0182】また、第二のKw管理部2706が第二のKwを第二のECM生成部2707へ送信し、第二のECM生成部2707は第二のECMを生成して変調部2710へ送信し、変調部2710は適切な変調を行い、周波数変換部2708へ送信し、周波数変換部2708では第二のECMをCATV回線106上の対応する周波数帯域に変換して混合部2709へ送信する。混合部2709は周波数変換されたストリームと第二のECMとを周波数多重してCATV回線106へ送出する。

【0183】その他のシステム構成は第1の実施の形態と同様であるので、図を流用して、以下、動作を説明する。

【0184】図28はCATV回線106における周波数配列を示す図の一例である。

【0185】図28に示すように、コンテンツを含むト

ランスポートストリームを伝送する周波数帯域と、第二のECMを伝送する周波数帯域とは別の帯域を設ける。

【0186】CATV局105において周波数変換部2705はコンテンツを含むストリームを対応する周波数へ変換し、周波数変換部2708は第二のECMを、コンテンツを含むストリームとは別の周波数帯域2801に変換して送出する。

【0187】CATV端末107は第二のECMを受信する場合に、必要に応じて第二のECM用の周波数帯域2801を受信するようにして、自分宛の第二のECMを受信し、契約情報などを保持する。コンテンツを視聴する場合には、該当するコンテンツが含まれるストリームを受信するようにして、該当コンテンツに対応する第二のECMを受信し、先に受信している第二のECMの契約情報と比較して、視聴判定を行うようにすればよい。

【0188】以上のように本実施の形態によれば、CATV局105において、周波数変換部2708が第二のECMを、コンテンツを含むストリーム用の周波数帯域とは別の周波数帯域を用いて送信するようにしたので、CATV局105はコンテンツを含むストリームの伝送容量を狭くすることなく、また、コンテンツに影響を与えることなく任意のタイミングで第二のECMを送信することができるという効果が得られる。

【0189】図29は本実施の形態におけるCATV端末107の内部構成の要部を示す図の別の例である。

【0190】このCATV端末107は、第二のECMを復調する復調部2908と、第二のECM用の周波数帯域2801を復調部2908に分配する分配部2901と、自分宛の第二のECMを抽出する第二のECM抽出部2909とを備えている。

【0191】このCATV端末107において、分配部2901はCATV回線106の信号から第二のECM用の周波数帯域2801を復調部2908に分配し、残りの信号をチューナ2902へ送信する。復調部2908は第二のECMの復調を行い、第二のECM抽出部2909へ送信し、第二のECM抽出部2909は自分宛の第二のECMを受信した場合に、限定受信モジュール2905へ自分宛の第二のECMを送信する。分離部2903はチューナ2902及び復調部2908を介して、視聴すべきコンテンツを含むストリームを受信し、第二のECMを限定受信モジュール2905へ送信する。限定受信モジュール2905は第二のECMを受信した場合は、契約情報やKwなどを保持しておき、第二のECMを受信した場合には、保持している契約情報を用いて視聴判定を行い、視聴可能であれば第二のECMに含まれているKsをデスクランブラ2906へ送信する。デスクランブラ2906はKsをもとにコンテンツのデスクランブルを行い、出力制御部2907へ送信し、出力制

部2907はコンテンツを出力する。

[0192] 以上のようにCATV端末107を構成すれば、分配部2901が第二のECMを分配して、復調部2908へ送信し、第二のECM抽出部2909を介して限定受信モジュール2905へ送信するので、チューナ2902がコンテンツを含むトランスポートストリームの周波数帯域を受信している場合に、任意のタイミングで第二のECMを受信することが可能となる。また、復調部2903とは別に、第二のECMを復調するための復調部2908を設けているので、コンテンツを含むトランスポートストリームの復調方式とは独立して任意の復調方式を採用することができる。例えば、コンテンツを含むトランスポートストリームの復調方式が84QAMであるとして、第二のECMの復調方式はPSK、QPSK、FSK、その他のQAMなど全く独立して復調を行うことが可能である。

[0193] (第8の実施の形態) 図30はCATV局105の内部構成の要部を示す図の一例である。

[0194] このCATV局105は、公衆網3004を通じて第二のECMをCATV端末107に送信しており、そのための通信部3003を具備している。

[0195] このCATV局105の第二のKw管理部3001は第二のKwを第二のECM生成部3002へ送信し、第二のECM生成部3002は第二のECMを生成して、通信部3003へ送信し、通信部3003はCATV回線106とは別の伝送路、例えば公衆網3004へ第二のECMを送信する。その他の構成は第7の実施の形態と同様であるので、流用して説明する。

[0196] 図31はCATV端末107の内部構成の要部を示す図の一例である。

[0197] このCATV端末107は通信部3101を有しており、CATV局105とCATV回線106及び公衆網3004に接続されている。CATV端末107において、通信部3101は公衆網3004から自発的に第二のECMを受信し、限定受信モジュール3109へ送信する。限定受信モジュール3109は、第二のECMを受信すると、第二のKw及び契約情報を保持し、分岐部3104から第二のECMを受信すると、保持している契約情報と比較して視聴判定を行い、視聴可能と判定すると第二のECMに含まれているKsをデスクランブラ3106へ送信する。

[0198] 以上のように、本実施の形態によれば、CATV局105では、通信部3003が第二のECMを公衆網3004へ送出し、CATV端末107では、通信部3101が公衆網3004から第二のECMを受信し、限定受信モジュール3109へ送信するようにしたので、CATV回線106上のコンテンツを含むトランスポートストリームに影響を及ぼさず、第二のECMを任意のタイミングで送信することが可能となる。また、CATV回線106に第二のECMを送信するための周波数帯域がない場合でも第二のECMの送信が可能である。

[0199] なお、本実施の形態では公衆網3004を用いるとしたが、これに限定するのではなく専用線や無線など様々な伝送手段を利用することが可能である。

[0200] (第9の実施の形態) 図32は放送センタ101の内部構成の要部を示す図の一例である。

[0201] この放送センタ101は、第二のECMを専用線CATV局105に送信しており、そのための通信部3204を具備している。

[0202] この通信部3204は、第二のECM生成部3202と接続され、さらに専用線3205を介してCATV局105と通信できるようになっている。第二のKw管理部3201は第二のKwを第二のECM生成部3202に送信し、サイマルクリプト制御部3203はKs生成部208より受信したKsを第一のECM生成部3204とともに第二のECM生成部3202に送信する。第二のECM生成部3202は受信したKs及び第二のKwを基に第二のECMを生成し、通信部3204へ送信し、通信部3204は専用線3205へ第二のECMを送信する。サイマルクリプト制御部3203は第一のECM生成部204より受信した第一のECMを多重部3206に送信するとともにスクランブラ210へKsを送信する。

[0203] 図33はCATV局105における多重部304の内部及び周辺構成を示す図の一例である。図33に示すようにCATV局105は通信部3303を有しており、通信部3303は専用線3205を介して放送センタ101に接続されている。CATV局105において、通信部3303は専用線3205から送られてくる第二のECMを受信し、共通情報多重装置3301へ送信する。共通情報多重装置3301は受信した第二のECMをコンテンツを含むトランスポートストリームに多重して多重装置3302へ送信し、多重装置3302は第二のECMをさらに多重して送信する。その他、図示していない要素は第1の実施の形態と同様であるので詳細は割愛する。

[0204] 以上のように構成される限定受信システムについて、以下、動作を説明する。放送センタ101は衛星回線102へコンテンツ、第一のECM及び第一のECMを含むトランスポートストリームを送信し、通信部3204によって第二のECMを専用線3205へ送信する。

[0205] CATV局105では、通信部3303が専用線3205から第二のECMを受信し、共通情報多重装置3301が、衛星回線102から受信したトランスポートストリームに、第二のECMを多重して送信する。

[0206] 以上のように、本実施の形態によれば、衛星回線102上には、直接受信端末104に不要である第二のECMが存在しないので、直接受信端末104の動作動作防止につながり、さらに、衛星回線102上の伝送容量を増加できるという効果が得られる。

[0207] また、図34は共通情報多重装置3301の動作を説明する図であり、第二のECMを多重する方法としては、図34に示すように、第一のECMと第二のECM

CMと入れ替えて多重するという方法がある。共通情報多重装置3301は1パケット以上のバッファを有しており、トランスポートストリームをバッファに蓄えながらパケットの種類をチェックし順次送出していく。また、通信部3303から受信した第二のECMを保持するバッファも1パケット以上有している。そして、第二のECMを保持している場合、トランスポートストリーム内に第一のECMを検出すると、保持している第二のECMと第一のECMとを入れ替えて送信する。このようにすれば、トランスポートストリームの伝送速度を変更することなく、第二のECMを多重することが可能となる。また、この場合は、第一のECMだけではなくヌルパケットや第一のECMと入れ替えて、第二のECMを多重するようにしても同様の効果が得られる。

[0208] また、第二のECMを保持していない場合に、第一のECMを検出したときは、ヌルパケットと入れ替えるようにしてもよい。このようにすれば、CATV端末107に不要な第一のECMをCATV回線106に送出することがなくなるので、CATV端末107の動作動作防止につながる。

[0209] なお、本実施の形態において、放送センタ101の第二のKw管理部3201と、CATV局105の第二のKw管理部307との間で第二のKwを共有する必要があるが、その方法としては、専用線3205を利用する方法がある。つまり、放送センタ101において、第二のKw管理部3201は通信部3204と接続されており、第二のKwを通信部3204を介して専用線3205へ送出する。また、CATV局105において、第二のKw管理部307は通信部3303に接続されており、専用線3205から通信部3303を介して第二のKwを受信するという方法がある。また専用線3205が双方向通信可能であるとすると、CATV局105から放送センタ101へ専用線3205を介して第二のKwを送信する方法もある。また、この場合に、放送センタ101に複数のCATV局105が接続されている場合は、ある1つのCATV局105から放送センタ101に専用線3205を介して第二のKwを送信し、放送センタ101がその他のCATV局105へ専用線3205を介して第二のKwを送信する方法もある。また、ある1つのCATV局105から放送センタ101及びその他のCATV局105へ専用線3205を介して第二のKwを送信する方法もある。

[0210] また、専用線3205で第二のKwを送信する際に、秘密鍵暗号方式や公開鍵暗号方式を利用するようにすれば、第二のKwの秘匿性を向上させることが可能となる。

[0211] なお、第二のKwの共有方法は、専用線3205を用いた方法、第1の実施の形態で説明した記憶媒体、衛星回線102及び公衆網を用いた方法の、いずれかの方法を組み合わせることが可能である。

[0212] (第10の実施の形態) 図35は限定受信システムの全体構成を示す図の一例である。

[0213] このシステムは、CATV端末107の視聴履歴を収集する第一の視聴履歴収集センタ3501と、第二の視聴履歴収集センタ3502とを備えている。CATV端末107は、公衆網3503を用いて通信するための通信部3504を有しており、第一の視聴履歴収集センタ3501及び第二の視聴履歴収集センタ3502は公衆網3503を介して、CATV端末107と接続されている。その他の構成は第1の実施の形態と同様であるので、流用して以下、動作を説明する。

[0214] CATV局105は第二のECMに第二の視聴履歴収集センタ3502の電話番号を格納して送信し、CATV端末107はその電話番号を保持しておく。放送センタ101はコンテンツの内容に応じて、必要があれば第二のECMに第一の視聴履歴収集センタ3501の電話番号を格納して送信する。CATV端末107はPPVで提供されるコンテンツを視聴した場合には、その視聴履歴を送信する必要があるが、本実施の形態においては図36に示すフローチャートのように送信する。すなわち、ステップ3601: 視聴したコンテンツに対応する第二のECMに第一の視聴履歴収集センタ3501の電話番号が格納されているかを判定する。もし電話番号があった場合には、

ステップ3602: 第一の視聴履歴収集センタ3501へ電話して視聴履歴を送信する。また、ステップ3603において、電話番号が無かった場合には、ステップ3603: 予め第二のECMで受信している第二の視聴履歴収集センタ3502の電話番号を用いて電話して視聴履歴を送信する。

[0215] 以上のように、本実施の形態によれば、第二のECMに格納されている電話番号を優先的に利用して視聴履歴を送信するので、コンテンツの内容に応じて、任意の場所で視聴履歴を収集することが可能となる。

[0216] なお、本実施の形態では、第二のECMに第二の視聴履歴収集センタ3502の電話番号を格納して送信するとして、CATV回線106が双方向通信可能であり、CATV局105が視聴履歴を収集する場合には、この電話番号は特に必要ではなく、電話番号を格納しない場合には、図36のステップ3603において、CATV回線106を利用して視聴履歴を送信するようにしてもよい。

[0217] (第11の実施の形態) 図37は限定受信システムの全体構成を示す図の一例である。

[0218] 放送センタ3701には、第二のECMを送出する1つ以上の第一のCATV局3703と、第NのECMを送出する1つ以上の第二のCATV局3706が接続され、第一のCATV局3703はCATV回線3704を介して1つ以上の第一のCATV端末3705に接続され、第二のCATV局3706はCATV回線3707を介して1つ以上の第二のCATV端末3708に接続されている。直接受

信端末3702は衛星回線102を介して放送センタ3701に接続されている。

【0219】図38は放送センタ3701の内部構成の要部を示す図の一例である。

【0220】放送センタ3701は、図2において説明した放送センタ101の構成に、さらに第NのKw管理部3807と第NのECM生成部3808とを有しており、第NのKw管理部3807は第NのKwを第NのECM生成部3808へ送信し、サイマルクリプト制御部3809はKsを第一のECM生成部3804、第二のECM生成部3805及び第NのECM生成部3808に送信する。第NのECM生成部3808は受信した第NのKw及びKsを基に、第NのECMを生成しサイマルクリプト制御部3809へ送信する。第一のECM生成部3804、第二のECM生成部3805もそれぞれ第一のECM及び第二のECMを生成しサイマルクリプト制御部3809へ送信し、サイマルクリプト制御部3809は第一のECM、第二のECM及び第NのECMを多重部3811へ送信し、Ksをスクランブラ3812へ送信する。その他の構成要素は第1の実施の形態で説明したものに相当するので、説明は割愛する。

【0221】図39は第二のCATV局の内部構成の要部を示す図である。

【0222】第二のCATV局3706は第NのKw管理部3907及び第NのECM生成部3908を有しており、その他の構成要素は図3で示した要素に対応するものとする。

【0223】第NのKw管理部3907は第NのKwを第NのECM生成部3908へ送信し、第NのECM生成部3908は第NのKwを基に第NのECMを生成して、多重部3904へ送信する。そしてコンテンツを含むトランスポートストリームに第NのECMを多重して、CATV回線3707に送出する。

【0224】第一のCATV局の内部構成は図3で説明した構成と同様とし、第二のECMを生成してコンテンツを含むトランスポートストリームに第二のECMを多重して、CATV回線3704に送出する。

【0225】以上の構成よりなる限定受信システムについて以下、動作を説明する。

【0226】放送センタ3701はコンテンツ、第一のECM、第一のECM、第二のECM及び第NのECMを衛星回線102へ送信し、第一のCATV局3703はCATV回線3704へコンテンツを含むトランスポートストリームに第二のECMを多重して送信するものとし、第二のCATV局3706はCATV回線3707へコンテンツを含むトランスポートストリームに第NのECMを多重して送信するものとする。第一のCATV局3703は第二のECM及び第二のECMを用いて視聴判定を行い、第二のCATV局3706は第NのECM及び第NのECMを用いて視聴判定を行う。直接受信端末3702は第一のECM及び第一のECMを用いて視聴判定を行う。

【0227】以上のように、本実施の形態によれば、放

送センタ3701から第一のECMの他に、第二のECM及び第NのECMを送信し、第一のCATV局3703は第二のECMを送信し、第二のCATV局3706は第二のECMを送信するようにしたので、各CATV局はそれぞれ独立して限定受信の運用を行うことができるという効果が得られる。

【0228】このようにすれば、さらに、複数のECMを放送センタ3701から送信し、各CATV局では自局の運用に適したECMを利用して限定受信を行うことが可能となり、より柔軟に独立して運用を行うことが可能となる。

【0229】なお、各Kwの共有方法としては別の実施形態で説明した、記憶媒体、衛星回線102、公衆網、さらに、放送センタ3701とCATV局を接続する専用線などを使用する方法が利用できる。なお、この場合には、例えば第二のKwを共有する場合には、第二のKwを利用しているCATV局にのみ送信するようにしてもよく、その他の各Kwについても同様であり、必要となるCATV局にのみ送信するようにしてもよい。

【0230】なお、全ての実施の形態において説明した図は全て要部のみを記述しており、本発明に必要なと思われる構成要素は割愛している。

【0231】また、全ての実施の形態は必要に応じて組み合わせることができることはいうまでもない。

【0232】また、全ての実施の形態において送信するトランスポートストリームは1つではなく、複数存在することはいうまでもない。

【0233】また、全ての実施の形態における衛星回線やCATV回線は特にそれに限定されるものではなく、CATV回線、衛星回線、専用線、無線、公衆網など様々な伝送路の適用が可能である。

【0234】

【発明の効果】以上の説明から明らかなように、本発明の限定受信システムは、次のような効果を有している。

【0235】CATV局は、CATV端末装置に対して、センタ装置からのコンテンツを簡単な構成で提供でき、低コスト化が図れるとともに、CATV局独自の限定受信を行うことができる。

【0236】また、センタ装置がCATV端末用のECMを専用線でCATV局に伝えるシステムでは、直接受信端末に不要なECMが衛星回線から除かれるので、直接受信端末の誤動作防止につながる。

【0237】また、CATV局が、受信したCATV端末用のECMを一定期間で繰り返し送出するシステムでは、その分、衛星回線での伝送容量をコンテンツなどの伝送に振り向けることが可能になり、コンテンツの更なる高画質化や、多チャンネル化といった効果が得られる。

【0238】また、CATV端末用ECMと直接受信端

末用ECMと異なる暗号化方式で暗号化することにより、CATV端末及び直接受信端末に対する限定受信を独立して行うことが可能となり、一方の暗号化方式が破られた場合にも、もう一方の限定受信には影響を及ぼすことがないという効果が得られる。

【0239】また、CATV端末用ECMと直接受信端末用ECMとのアクセス判定領域の構成を別々にすることにより、CATV端末及び直接受信端末に対する限定受信を独立して行うことが可能となり、一方のアクセス判定領域の構成が見破られて改竄された場合でも、もう一方の限定受信には影響を及ぼすことがないという効果が得られる。

【0240】また、CATV局がCATV端末用ECMにアクセス判定領域を通知し、これを第三のワーク鍵で暗号化することにより、CATV端末に対する限定受信をさらに独立して行うことが可能となるとともに、CATV端末用ECMの秘匿性を確保できるという効果が得られる。

【0241】また、CATV局が、受信ストリームから直接受信端末用のECMやECMを取り除き、あるいは、CATV端末用のECMやECMを入れ替えて中継することにより、CATV回線に送出する情報の伝送容量を増加できるという効果が得られる。

【0242】また、CATV局が、コンテンツを含む情報を中継する周波数帯域とは別の周波数帯域でCATV端末用ECMを送信することにより、コンテンツを含む情報の伝送容量に影響を及ぼすことなく、任意の伝送容量でCATV端末用ECMを送信できるという効果が得られる。

【0243】また、ティア番組またはペイパービュー番組を示す番組属性をCATV局が設定できるようにすることにより、CATV端末に対する限定受信を独立して行うことができるという効果が得られる。

【0244】また、本発明のシステムでは、センタ装置とCATV局との間でCATV端末用のワーク鍵を簡単に共有できるという効果が得られる。

【0245】また、CATV局が主体的にCATV端末用のワーク鍵の変更を行うことができるという効果が得られる。

【0246】また、端末装置の視聴履歴を任意の視聴履歴収集先で収集することができるという効果が得られる。

【0247】なお、ここではCATV局に特化して説明したが、本発明は、他の中継装置に対しても適用が可能であり、その場合にも、同様の効果を得ることができる。

【図面の簡単な説明】

【図1】本発明の第1の実施の形態における限定受信システムの全体構成図。

【図2】本発明の第1の実施の形態における放送センタ

の内部構成図。

【図3】本発明の第1の実施の形態におけるCATV局の内部構成図。

【図4】本発明の第1の実施の形態における直接受信端末の内部構成図。

【図5】本発明の第1の実施の形態におけるCATV端末の内部構成図。

【図6】本発明の第1の実施の形態におけるECMの基本構成図。

【図7】本発明の第1の実施の形態におけるECMの基本構成図。

【図8】本発明の第1の実施の形態における限定受信モジュールの動作を示す図。

【図9】本発明の第1の実施の形態における視聴判定ティアビットの構成図。

【図10】本発明の第1の実施の形態における契約情報ティアビットの構成図。

【図11】本発明の第1の実施の形態における契約判定ビットマップの構成図。

【図12】本発明の第1の実施の形態における契約判定ビットマップの構成図。

【図13】本発明の第2の実施の形態における多重部の内部構成図。

【図14】MPEG2トランスポートストリームパケットのヘッダ部の要部を示す図。

【図15】本発明の第2の実施の形態におけるECMの基本構成図。

【図16】本発明の第3の実施の形態における多重部の内部構成図。

【図17】本発明の第3の実施の形態におけるECMの基本構成図。

【図18】本発明の第3の実施の形態における多重装置の動作を示す図。

【図19】本発明の第4の実施の形態における多重部の内部構成図。

【図20】本発明の第4の実施の形態における個別情報多重装置の動作を示す図。

【図21】本発明の第5の実施の形態における多重部の内部構成図。

【図22】本発明の第5の実施の形態における共通情報多重装置の動作を示す図。

【図23】本発明の第5の実施の形態における第二のECMの構成図。

【図24】本発明の第8の実施の形態における第二のECMの構成図。

【図25】本発明の第8の実施の形態における第二のECMの構成図。

【図26】本発明の第8の実施の形態における第二のECMの構成図。

【図27】本発明の第7の実施の形態におけるCATV

局の内部構成図。

【図28】本発明の第7の実施の形態におけるCATV回線上の周波数帯域を示す図。

【図29】本発明の第7の実施の形態におけるCATV端末の内部構成図。

【図30】本発明の第8の実施の形態におけるCATV局の内部構成図。

【図31】本発明の第8の実施の形態におけるCATV端末の内部構成図。

【図32】本発明の第9の実施の形態における放送センタの内部構成図。

【図33】本発明の第9の実施の形態におけるCATV局の多重部の内部及び周辺の構成図。

【図34】本発明の第9の実施の形態における共通情報多重装置の動作を示す図。

【図35】本発明の第10の実施の形態における限定受信システムの全体構成図。

【図36】本発明の第10の実施の形態におけるCATV端末の動作を示す図。

【図37】本発明の第11の実施の形態における限定受信システムの全体構成図。

【図38】本発明の第11の実施の形態における放送センタの内部構成図。

【図39】本発明の第11の実施の形態における第二のCATV局の内部構成図。

【図40】従来のパスルー方式を説明する図。

【図41】従来のサイマルクリプト方式を説明する図である。

【符号の説明】

101、3701 放送センタ

104、3702 直接受信端末

105 CATV局

107 CATV端末

202、3803 第一のEMM生成部

204、3804 第一のECM生成部

* 205、3202、3806 第二のECM生成部

206、3201、3805 第二のKw管理部

207、3203、3809 サイマルクリプト制御部

303、2703、3903 PSI変換部

304、3904 多重部

305、2704、3905 QAM変調部

306、2705、3906 周波数変換部

307、2706、3001 第二のKw管理部

308、2707、3002 第二のEMM生成部

404、504、2904、3104 分路部

405、505、2905、3105 限定受信モジュール

1301 共通情報除去装置

1302、1602、2102、3302 多重装置

1501 ECM識別子

1601 個別情報除去装置

1701 EMM識別子

1901 個別情報多重装置

2101、3301 共通情報多重装置

2301 番組属性

2710 変調部

2708 周波数変換部

2901 分配部

2909 第二のEMM抽出部

3003 通信部

3011 通信部

3004 通信部

3303 通信部

3501 第一の視聴履歴収集センタ

3502 第二の視聴履歴収集センタ

3703 第一のCATV局

3705 第一のCATV端末

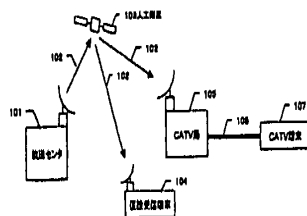
3706 第二のCATV局

3708 第二のCATV端末

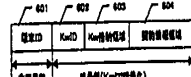
3907 第NのKw管理部

* 3908 第NのEMM生成部

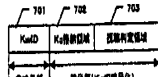
【図1】



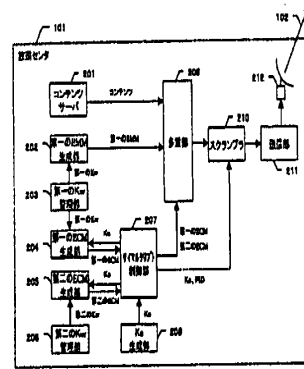
【図6】



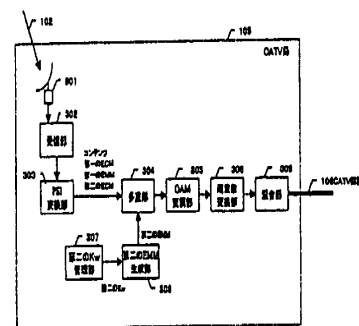
【図7】



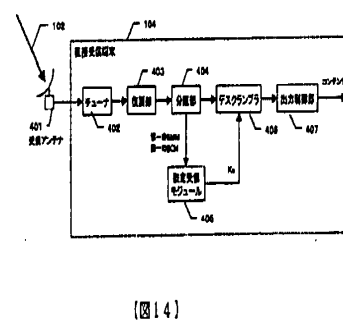
【図2】



【図3】



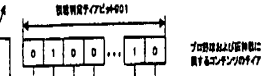
【図4】



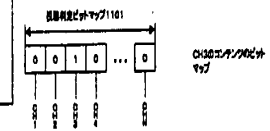
【図14】



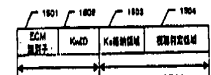
【図9】



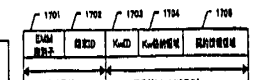
【図11】



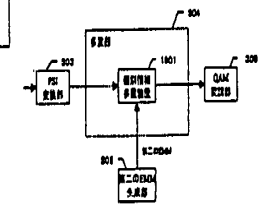
【図15】



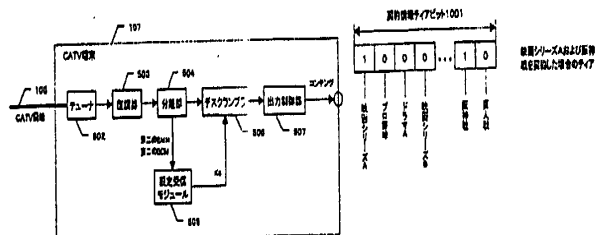
【図17】



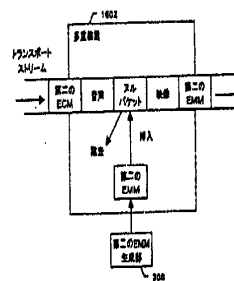
【図19】



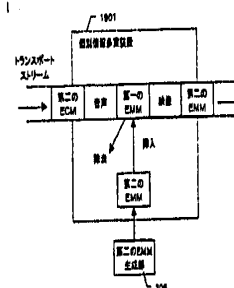
【图5】



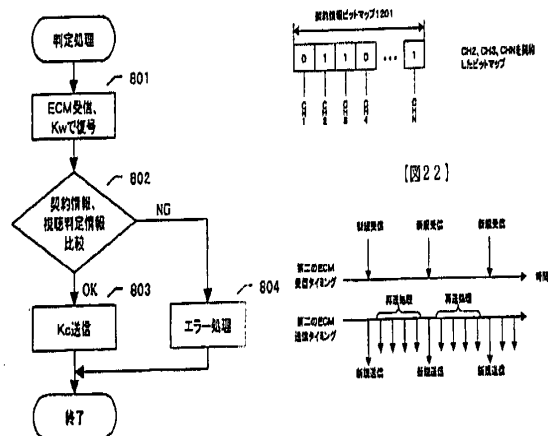
【图10】



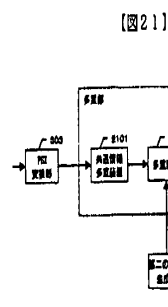
【图20】



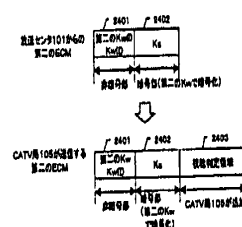
【圖8】



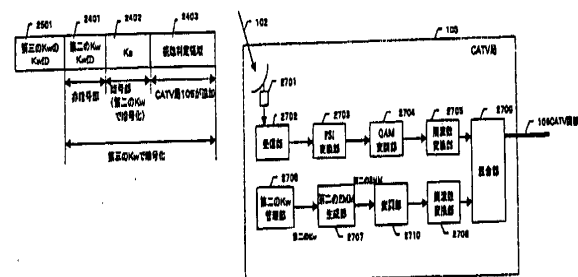
【图22】



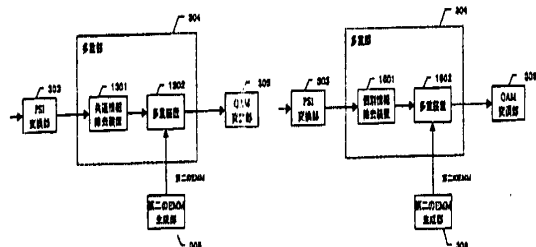
【图24】



【例25】

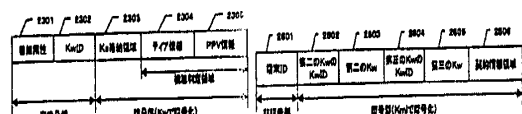


【例 13】

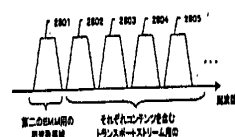


【图16】

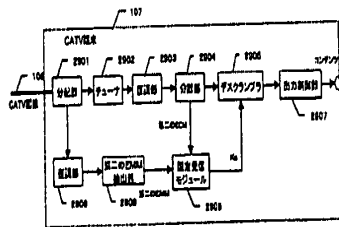
【例23】



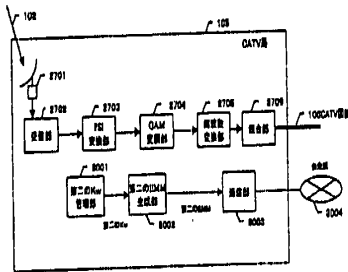
【圖26】



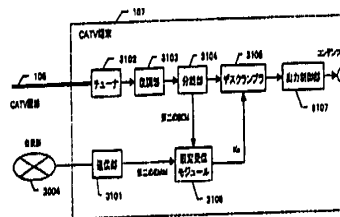
【図29】



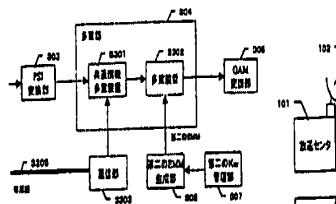
【図30】



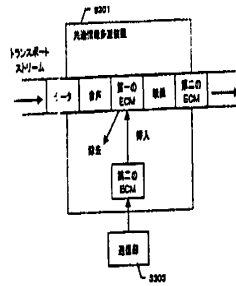
【図31】



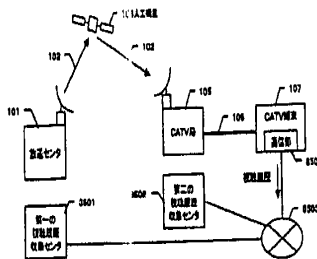
【図33】



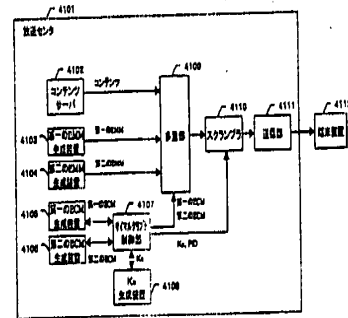
【図34】



【図35】



【図41】



フロントページの続き

(72)発明者 櫻井 厚典

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72)発明者 内藤 康文

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

(72)発明者 後藤 吉正

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

Fターム(参考) SC064 CA14 CB01 CC01 CC04

S1104 AA01 AA16 BA02 BA03 EA04

EA06 EA17 JA03 NA03 PA04

PA06